

BEST AVAILABLE COPY

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/US04/017756

International filing date: 04 June 2004 (04.06.2004)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/475,639
Filing date: 04 June 2003 (04.06.2003)

Date of receipt at the International Bureau: 19 August 2004 (19.08.2004)

Remark: Priority document submitted or transmitted to the International Bureau in
compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

1209519

'ND AND TO WILSON THOMAS PRESENIS, SHAW, COMPT.

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

August 10, 2004

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM
THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK
OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT
APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A
FILING DATE.

APPLICATION NUMBER: 60/475,639

FILING DATE: June 04, 2003

RELATED PCT APPLICATION NUMBER: PCT/US04/17756

Certified by

Jon W Dudas

Acting Under Secretary of Commerce
for Intellectual Property
and Acting Director of the U.S.
Patent and Trademark Office





BAKER BOTTS LLP

Please type a plus sign (+) inside this box →

Attorney Docket No. P35860
Express Mail Label No. EV342491873US

APDien
PTO

17602 U.S. PTO
60/475639
06/04/03

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

INVENTOR(S)			
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)	
Bruce	Rutherford	Stamford, CT	
Alfred	Dagher	Wyckoff, NJ	
Mark	Wiesman	Chesterfield, MO	
<input checked="" type="checkbox"/> Additional inventors are being named on the _____ separately numbered sheets attached hereto			
TITLE OF THE INVENTION (280 characters max)			
METHOD AND SYSTEM FOR REMOTE CARDHOLDER AUTHENTICATION USING A CHIP CARD			
Direct all correspondence to:			
CORRESPONDENCE ADDRESS			
<input checked="" type="checkbox"/> Customer Number	21003	→ Place Customer Number Bar Code Label here	
OR	Type Customer Number here		
<input type="checkbox"/> Firm or Individual Name			
Address			
Address			
City	State	ZIP	
Country	Telephone	Fax	
ENCLOSED APPLICATION PARTS (check all that apply)			
<input checked="" type="checkbox"/> Specification Number of Pages	136	<input type="checkbox"/> CD(s), Number	
<input type="checkbox"/> Drawing(s) Number of Sheets		<input type="checkbox"/> Other (specify)	
<input type="checkbox"/> Application Data Sheet. See 37 CFR 1.76			
METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT			
<input type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27.	FILING FEE AMOUNT (\$)		
<input checked="" type="checkbox"/> A check or money order is enclosed to cover the filing fees			
<input type="checkbox"/> The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number:	02-4377	160	
<input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.			
The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.			
<input checked="" type="checkbox"/> No.			
<input type="checkbox"/> Yes, the name of the U.S. Government agency and the Government contract number are: _____			

Respectfully submitted,

SIGNATURE

TYPED or PRINTED NAME Robert C. Scheinfeld

TELEPHONE 212-408-2512

Date: June 4, 2003

REGISTRATION NO.
(if appropriate)

31,300

Docket Number:

P35860

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

60475639 , 060403

BAKER BOTTS LLP

PROVISIONAL APPLICATION COVER SHEET

Additional Page

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

60475639 . 060403

BAKER BOTTS LLP

FEE TRANSMITTAL for FY 2003

Effective 01/01/2003. Patent fees are subject to annual revision.

 Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT (\$ 160)

Complete If Known

Application Number	
Filing Date	
First Named Inventor	Bruce Rutherford
Examiner Name	
Art Unit	
Attorney Docket No.	P35860

METHOD OF PAYMENT (check all that apply)

Check Credit card Money Order Other None

Deposit Account:

Deposit Account Number 02-4377
Deposit Account Name Baker Botts LLP

The Commissioner is authorized to: (check all that apply)
 Charge fee(s) indicated below Credit any overpayments
 Charge any additional fee required under 37CFR 1.16 and 1.17
 Charge fee(s) indicated below, except for the filing fee to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code (\$)	Small Entity Fee Code (\$)	Fee Description	Fee Paid
1001 750	2001 375	Utility filing fee	
1002 330	2002 165	Design filing fee	
1003 520	2003 260	Plant filing fee	
1004 750	2004 375	Reissue filing fee	
1005 160	2005 80	Provisional filing fee	160

SUBTOTAL (1) (\$ 160)

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

Total Claims	- 20 =	0	X	Fee from below	Fee Paid
Independent Claims	- 3 =	0	X		0
Multiple Dependent					

Large Entity Fee Code (\$)	Small Entity Fee Code (\$)	Fee Description	Fee Paid
1202 18	2202 9	Claims in excess of 20	
1201 84	2201 42	Independent claims in excess of 3	
1203 280	2203 140	Multiple dependent claim, if not paid	
1204 84	2204 42	** Reissue independent claims over original patent	
1205 18	2205 9	** Reissue claims in excess of 20 and over original patent	

SUBTOTAL (2) (\$ 0)

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code (\$)	Small Entity Fee Code (\$)	Fee Description	Fee Paid
1051 130	2051 65	Surcharge - late filing fee or oath	
1052 50	2052 25	Surcharge - late provisional filing fee or cover sheet	
1053 130	1053 130	Non-English specification	
1812 2,520	1812 2,520	For filing a request for ex parte reexamination	
1804 920*	1804 920*	Requesting publication of SIR prior to Examiner action	
1805 1,840*	1805 1,840*	Requesting publication of SIR after Examiner action	
1251 110	2251 55	Extension for reply within first month	
1252 410	2252 205	Extension for reply within second month	
1253 930	2253 465	Extension for reply within third month	
1254 1,450	2254 725	Extension for reply within fourth month	
1255 1,970	2255 985	Extension for reply within fifth month	
1401 320	2401 160	Notice of Appeal	
1402 320	2402 160	Filing a brief in support of an appeal	
1403 280	2403 140	Request for oral hearing	
1451 1,510	1451 1,510	Petition to institute a public use proceeding	
1452 110	2452 55	Petition to revive - unavoidable	
1453 1,300	2453 650	Petition to revive - unintentional	
1501 1,300	2501 650	Utility issue fee (or reissue)	
1502 470	2502 235	Design issue fee	
1503 630	2503 315	Plant issue fee	
1460 130	1460 130	Petitions to the Commissioner	
1807 50	1807 50	Processing fee under 37 CFR 1.17(q)	
1806 180	1806 180	Submission of Information Disclosure Stmt	
8021 40	8021 40	Recording each patent assignment per property (times number of properties)	
1809 750	2809 375	Filing a submission after final rejection (37 CFR 1.129(a))	
1810 750	2810 375	For each additional invention to be examined (37 CFR 1.129(b))	
1801 750	2801 375	Request for Continued Examination (RCE)	
1802 900	1802 900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) (\$ 0)

(Complete if applicable)

SUBMITTED BY	Name (Print/Type)	Registration No. /Attorney/Agent	Telephone
Signature	Robert C. Scheinfeld	31,300	212-408-2512

Date June 4, 2003

CERTIFICATION UNDER 37 C.F.R. 1.8(a) OR 1.10*

(When using Express Mail, the Express Mail label number is mandatory; Express Mail Certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

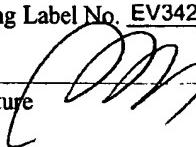
MAILING

deposited with the United States Postal Service in an envelope addressed to the
Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. 1.8(a)

with sufficient postage as first class mail.

as "Express Mail Post Office to Address"
Mailing Label No. EV342491873US (mandatory)

Signature 

Date: June 4, 2003

Robert C. Scheinfeld
(type or print name of person certifying)

***WARNING:** *Each paper office filed by "Express Mail" must have the number of the "Express Mail" mailing label placed thereon prior to mailing 37 C.F.R. 1.10(b). Since the filing of correspondence under § 1.10 without the Express Mail label thereon is an oversight that can be avoided by the exercise of reasonable care, requests for waiver of this requirement will not be granted on petition. "Notice of Oct. 24, 1996, 60 Fed. Reg. 56,439, at 56,442.*

CONFIDENTIAL

U.S. PROVISIONAL PATENT APPLICATION

“REMOTE CARDHOLDER AUTHENTICATION USING A CHIP CARD”

Inventors:

1. Bruce Rutherford
20 Glendale Road
Stamford, CT 06906
USA
Citizenship: USA
2. Alfred Dagher
294 Wiley Place
Wyckoff, NJ 07481
USA
Citizenship: USA
3. Mark Wiesman
1801 York Ridge Court
Chesterfield, MO 63017
USA
Citizenship: USA
4. Didier Jean Marie Charles Paie
Avenue Georges Marchal 22/301
1330 Rixensart
Belgium.
Citizenship: Belgium
5. Jean-Paul Edmond Rans
45 route d'Ottignies, B1380 Lasnes
Belgium
Citizenship : Belgium.
6. Fikret Ates
50, Rue Francois Dufer

CONFIDENTIAL

Assignee:

**MasterCard International Incorporated
2000 Purchase Street
Purchase, NY 10577**

CONFIDENTIAL

1

Overview

This chapter provides a high-level overview to the MasterCard SecureCode™ chip authentication programme. It identifies the role of this option in the overall MasterCard SecureCode program and the documents that provide the details of the specification for topics not covered in this document.

Overview

Introduction	1
MasterCard SecureCode Program.....	1
Scope of Specification.....	1
Business Requirements	1
Functional Overview	3
Entities.....	3
Authentication Request Server.....	3
Cardholder's PC Device.....	3
Cardholder.....	3
SecureCode™ Authentication Application.....	3
Personal Card Readers.....	4
The Process.....	4
Prerequisites	4
Typical Flow.....	5
Connected Personal Card Reader.....	8
Security Considerations	10
Overview	10
Proof of Cardholder Presence.....	10
Proof of Transaction Approval.....	11
Replay Protection	11
PIN Security.....	12
AC truncation.....	12
Summary of Security Requirements	12

Introduction

MasterCard SecureCode Program

MasterCard International has developed the MasterCard SecureCode™ program to offer flexible, robust and easy to implement solutions for cardholder authentication for electronic commerce. This program enables issuers to choose from a broad array of security solutions for authenticating cardholders. These solutions include the PC Authentication Program, Chip Authentication Program, and MasterCard's implementation of 3-D Secure.

Scope of Specification

This document describes the MasterCard SecureCode™ Chip Authentication Program to be used as a cardholder authentication option under the MasterCard SecureCode™ Program. This provides an EMV-based authentication application for the cardholder to use for remote authentication and is separate from the EMV payment application which is designed for face-to-face transactions. The application is used with a Personal Card Reader (PCR) to provide the cardholder with a dynamic SecureCode for one-time use.

Business Requirements

The global model for SecureCode™ Chip Authentication is based on the following business requirements, the overall objective being the implementation of a trusted mechanism for the authentication of e-commerce payment and issuer services:

- There must be information relating to cardholder presence for transactions that are online to the issuer.
- The solution must be based on standard EMV chip technology.
- The traditional authorization route through the payment system network must be used for payment transaction authorization.
- The solution must be able to work under the 3-D Secure version 1.0.2 infrastructure for end-to-end interoperability between merchant, acquirer and issuer systems, all of which must support the 3-D Secure infrastructure.
- The solution must use a Personal Card Reader (PCR) operating either as a stand-alone device or connected to the cardholder's access device (e.g. PC or PDA). The card reader must have a display and keypad to enable limited cardholder interaction.
- The inconvenience to the cardholder in using this solution must be kept to a minimum, but balanced against the security needs of the solution.

Overview**Introduction**

-
- The specifications for the Personal Card Reader should aim to support the maximum possible card implementations while at the same time catering for cardholder convenience.
 - Connected Personal Card Readers must be type-approved by MasterCard in order to bear the debit/credit brand. These readers provide for the protection of the PIN during the PIN-entry process.
 - The display on the Personal Card Reader must be capable of showing the PIN validation result and, for unconnected devices, displaying a SecureCode™ to be entered on the PC or PDA.
 - The cardholder must be notified when an incorrect PIN is entered and must be given the option to re-enter the PIN. The number of remaining PIN tries must be displayed to the cardholder.
 - The SecureCode™ will not be created unless the cardholder PIN has been verified by the ICC.
 - The Personal Card Reader must be capable of obtaining an indication of the data format that must be used to create the SecureCode™ from the IOC.
 - The Cardholder Authentication Page must be controlled from the issuer's Authentication Request Server with no preinstalled software required.
 - The cardholder must be capable of determining from the displayed interface an indication from the issuer as to whether or not to enter a challenge in the PCR. When such an indication is made, the reader must be capable of allowing the cardholder to enter the challenge and must include the challenge in the computation of the SecureCode™.

Functional Overview

Entities

Authentication Request Server

An Authentication Request Server provides an Authentication request service to another entity/component in a Web server environment, independent of that entity. The cardholder must be authenticated to the Authentication Request Server which can return an indication of the authentication result to the requesting entity. An Authentication Request Server can therefore adapt and evolve to different e-commerce environments and needs.

Cardholder's PC Device

The cardholder's Personal Computing Device is the computer platform on which they are performing the activity that requires them to be authenticated. When connected readers are used this will typically be a PC platform, however when using unconnected readers, this can be any device that is capable of accessing the Internet.

Cardholder

The cardholder posses a MasterCard smartcard payment card and a Personal Card Reader. A cardholder must enter their PIN into their PCR in order that a SecureCode™ may be generated and supplied to the Authentication Request Server for validation.

SecureCode™ Authentication Application

The SecureCode™ Authentication Application (SCAA) resides on the multi-application MasterCard card alongside the standard payment application. To reduce cost of development, the SCAA is a separate instance of the payment application, which provides the issuer with the ability to use a separate security environment for payments and remote authentications.

The application supports both the generation of a "one-time passcode" and the creation of a "proof of transaction acceptance" code. At their discretion and liability, issuers may also choose to use the application for cardholder authentication for other services.

The Authentication Application carries data that tells the Personal Card Reader how the Issuer expects the SecureCode™ to be constructed and so allows a single reader design to support the widest possible range of cards, even among the same issuer.

Overview

Functional Overview

Personal Card Readers

A Personal Card Reader is a low cost handheld smartcard reader with a numeric keypad and a display. The Personal Card Reader interacts with the cardholder and the IOC to produce a SecureCode.

Unconnected Readers

Personal Card Readers can be completely standalone, requiring no physical connection to the cardholder's personal computing device. Cardholders equipped with such readers must manually transfer all data between the reader and the PC device.

Connected Readers

Personal Card Readers may also be equipped with a connection to the cardholder's personal computing device. Cardholders equipped with such devices need only enter their PIN on the PCR to conduct the authentication process as the SecureCode™ is passed to the user interface on their computing device. A connected reader can behave as an unconnected reader if no connection is available.



Since both types of reader generate the same type of SecureCode™ Authentication Request Servers validate the SecureCode™ in exactly the same manner.

The Process

Prerequisites

An Authentication Request Server interacts with a cardholder through the medium of the HTML page. It is therefore assumed that the request for authentication has resulted from a HTTP query of some sort that is capable of processing HTML in the response which will be returned by the Authentication Request Server Extension.

The following data is required to be supplied in the request for the authentication request service;

- PAN – The PAN of the card to be used in the authentication process
- Cardholder's Personal Assurance Message – Cardholders enrolled into the SecureCode™ programme are required to supply a Personal Assurance Message which will be displayed when asked to authenticate.
- Transaction Details – Details of the transaction for which authentication is being requested must be displayed to the cardholder, whether payment for goods from a website or to obtain access to a bank account.

Overview
Functional Overview

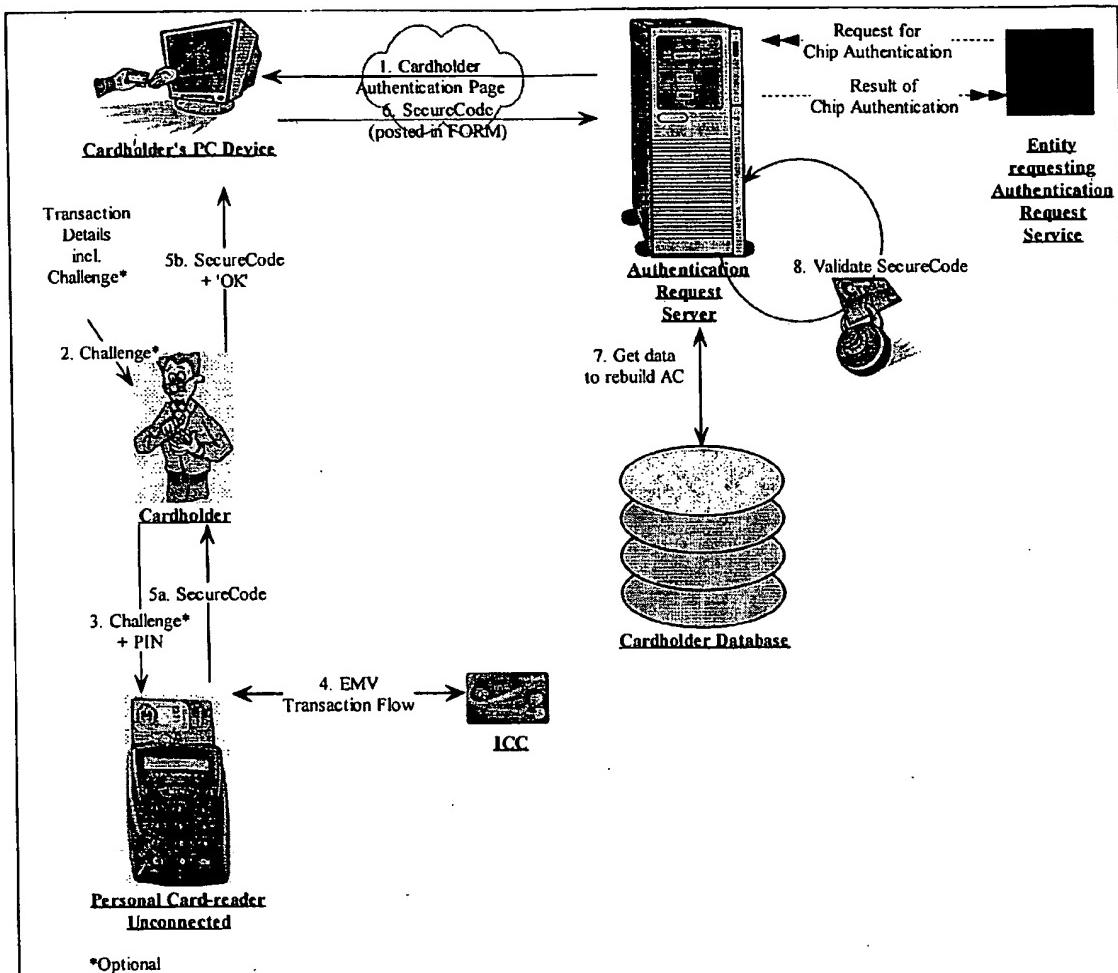
Typical Flow

Figure 1 Cardholder Authentication using an Unconnected Reader

1. Generation of Cardholder Authentication Page: Authentication Request Server to Cardholder (HTML)

In response to a request for authentication, the Authentication Request Server generates a HTML Cardholder Authentication Page. The page displays any details of the transaction as supplied by the requesting entity. The PAN is displayed as three groups of XXXX, with last 4 genuine PAN digits to help the cardholder ensure that they use the correct card to authenticate. The cardholder's Personal Assurance Message (PAM), supplied when the cardholder enrolled into the SecureCode™ program, is also displayed.

Overview**Functional Overview****2. Request SecureCode™: Cardholder's Browser**

The cardholder is prompted to insert their card into the PCR to create the SecureCode. When a challenge is utilized by the issuer, the cardholder is prompted to first enter the displayed challenge and to then press the OK button. If no challenge is provided, the cardholder must be appropriately educated to just press the OK button.

3. Enter PIN: Cardholder

The reader prompts the cardholder to enter their PIN and press the OK button.

Notes

If the PIN is not entered correctly, then the cardholder is prompted to re-enter the PIN. The number of PIN retries is displayed to the cardholder. The cardholder will be allowed no more than three tries.

If the PIN can not be entered correctly, then the transaction is rejected.

4. EMV Transaction Flow: PCR to ICC (APDU Command/Response)

The PCR conducts an optimised EMV transaction dialogue with the card to generate an application cryptogram – an ARQC.

Note

An ARQC is requested, but the card's own internal risk management may actually cause it to generate an AAC. However, since this is not a chip payment transaction, either type of cryptogram is acceptable.

5. Transfer SecureCode: PCR to Cardholder – Cardholder to HTML Form

5a. The response from the card is transformed by the PCR into a numerical SecureCode of 8 digits and is displayed on the reader.

5b. The SecureCode is read by the cardholder and is entered into the HTML page by the cardholder.

6. Submission of SecureCode™: Cardholder to Authentication Request Server (HTTPS/POST)

Once the HTML page has received the SecureCode and the cardholder has pressed Submit/OK, the SecureCode is sent to the Authentication Request Server for validation.

7. Retrieve Card Data: Authentication Request Server

The card specific static & dynamic data must be retrieved from a card database.

Note

The card specific dynamic data is the Application Transaction Counter (ATC). A copy of the last known ATC is kept in the card database so that the full ATC can be correctly rebuilt in combination with the partial ATC (lower bits) returned in the SecureCode.

8. Validate SecureCode: Authentication Request Server

The Authentication Request Server validates the SecureCode™ by rebuilding the input data used in the generation of the cryptogram by the ICC. This includes known static data, the

Overview

Functional Overview

transaction specific data (challenge) that was submitted to the ICC by the PCR and the data retrieved from the card database.



If no challenge was used, then the PCR will have used a default value of 0 for the Unpredictable Number.

The application cryptogram (ARQC/AAC) is recomputed and then is compared with the partial AC in the SecureCode. If they match, the ATC value is updated in the card database.



A process of partial cryptogram comparison is required, based on the format identified by the card's IIPB.

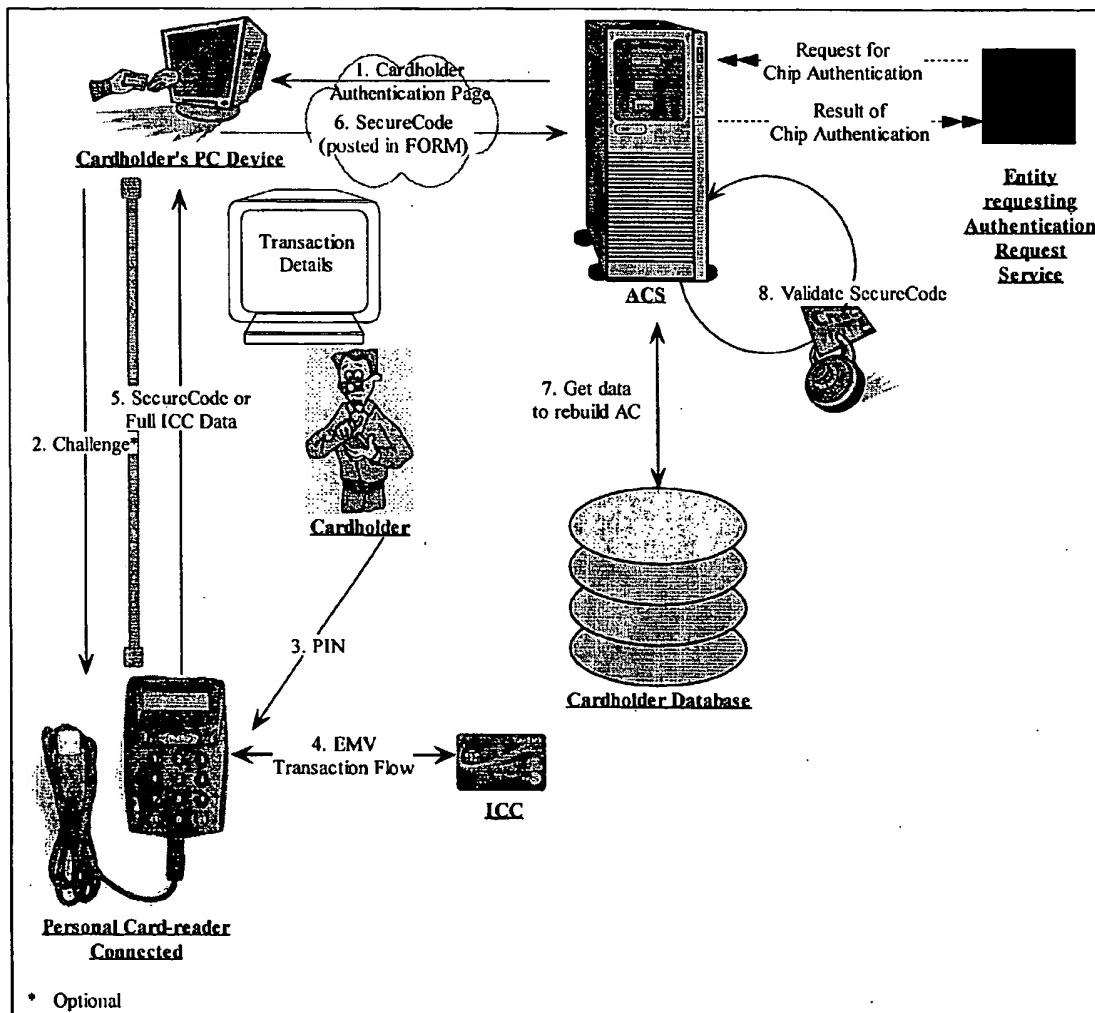
On completion of the authentication process, the Authentication Request Server returns an appropriate response to the entity requesting the authentication.

Overview**Functional Overview****Connected Personal Card Reader**

If a connected reader is used, the only differences are that any challenge is sent directly to the reader by an embedded software component referenced in the HTML page. The SecureCode is automatically entered into the proper data field after the cardholder has entered their PIN and the card has verified the PIN.

The SecureCode™ is processed by the Authentication Request Server in the same way for either type of reader.

The biggest change is to the cardholder since they will only need to insert their card and enter their PIN when prompted to do so.



601475639 · 060403

Overview
Functional Overview

Figure 2 Cardholder Authentication using a Connected Reader

Overview**Security Considerations**

Security Considerations

Overview

EMV security features provide the basis for the security of SecureCode™ chip authentication.

More specifically, SecureCode™ chip authentication relies on the generation of cryptograms by the ICC, namely the Application Cryptogram (AC) to establish:

- proof of card and cardholder presence for a one-time passcode
- proof of transaction approval by the cardholder by use of a challenge.

In addition, the use of cryptograms offers protection against the replay¹ of genuine transactions and the generation of fraudulent transactions.

Therefore, when used in conjunction with suitable security measures – especially related to PIN security – SecureCode™ chip authentication offers an adequate level of security to enforce the non-repudiation by the cardholder of transactions originated via the Internet.

Proof of Cardholder Presence

The ICC establishes proof of cardholder presence by the use of offline PIN validation. EMV specifications require that offline PIN validation is performed before the generation of an AC. Consequently, cardholder presence is required to generate a valid AC, and the existence of a valid cryptogram is sufficient to demonstrate cardholder presence. The AC is usually based on the ARQC, but may be based on the AAC should the card's internal risk management decide to decline what it believes is a payment transaction².


Warning

ICCs that do not include the CVR as part of the input data used for the AC calculation, both ARQC & AAC, can not be used in the context of this scheme.

¹ The repeated submission of previously submitted authentication data.

² A decline still serves our purpose as we are reusing a payment application just to get an Application Cryptogram.

Proof of Transaction Approval

The proof of the acceptance or approval of a transaction by the cardholder is based on the use of data provided by the Authentication Request Server in the cryptogram. This data is used as the Unpredictable Number (UN). For an unconnected reader, the challenge, when utilized, is used as the UN. The Authentication Request Server supplies the challenge to the connected reader. The challenge is a numeric value that is developed from information known only to the Authentication Request Server and which is whatever data the issuer feels is pertinent (e.g. the transaction amount and currency code.)

The use of a challenge provides the issuer and Authentication Request Server with the proof that the cardholder did approve that specific transaction because the displayed challenge is included in the cryptogram and the cryptogram is included in the SecureCode. A different challenge will produce a different SecureCode and there is no predictable way to know what challenge could be used to create a specific SecureCode.

Replay Protection

In order to ensure protection against fraudulent replays of genuine transactions, two conditions must be fulfilled:

- The issuer must check the Application Transaction Counter (ATC) received from the ICC against the last received ATC for that particular ICC. Transactions using an already received ATC must be declined.
- The AC generated by the ICC must vary as a function of the ATC. This is the case only when the ATC is included as part of the input data used for AC calculation. However, according to MasterCard's Minimum Card Requirements and ICC Application Specifications, such behavior, though recommended, is not mandatory to comply with EMV specifications.



Warning

ICCs that do not include the ATC as part of the input data used for the AC calculation *can not be used in the context of this scheme.*

Overview**Security Considerations**

PIN Security

The main security issue associated with the use of a Personal Card Reader device is the risk of disclosure of the PIN by the device itself. Fraudulent or tampered Personal Card Readers may endanger the confidentiality of this data. The level of risk depends on the type of device:

- **Unconnected Personal Card Reader** – The stand-alone nature of an unconnected reader allows these devices to be physically accessed by malicious parties wanting to gain access to confidential information. Only small-scale attacks are feasible on such devices and therefore the impact of such attacks is expected to be low.
- **Connected Personal Card Reader** – One-way or two-way connected readers offer more possibilities for fraud, due to the presence of a physical connection. Large-scale attacks could be feasible for such devices and therefore the impact of such attacks is expected to be higher.

AC truncation

The AC returned by the ICC is not transferred to the issuer in its entirety. Each cryptogram is truncated, as specified by the Issuer Internet Proprietary Bitmap (IIPB). The IIPB must be defined, by the issuer, in such a way that 16 bits from the AC are included in the SecureCode returned by the Personal Card Reader.

Because of the reduced size of truncated cryptograms, MasterCard recommends that issuers implement fraud detection systems to detect abnormal numbers of failed cryptogram validations, and take any appropriate action.

Summary of Security Requirements

Table 1.1 summarizes the security issues described in this section.

Table 1.1— Summary of Security Requirements for SecureCode™ Chip Authentication

Function	Requirements
-----------------	---------------------

Overview
Security Considerations

Function	Requirements
Cryptogram Calculation	<p>The card used must include the following data objects as part of the input data used for calculating the Application Cryptogram (AC):</p> <ul style="list-style-type: none"> • Card Verification Results (CVR) • Unpredictable Number (UN) <p>Applications that do not use these data objects as input to the cryptogram calculation, both ARQC & AAC, can not be used for chip authentication.</p>
Replay Protection	<p>Cryptograms must vary as a function of the ATC.</p> <p>Issuers must decline transactions that use an already received ATC.</p>
Fraud Detection	<p>MasterCard recommends that issuers implement fraud detection systems to detect abnormal numbers of failed cryptogram validations.</p>

2

Functional Requirements – Authentication Request Server

This chapter describes the functional requirements that apply to Internet based servers requesting authentication of cardholders equipped with an EMV card and a Personal Card Reader.

Functional Requirements – Authentication Request Server

Introduction	1
Responsibilities of an Authentication Request Server	1
\ Modifications to Standard 3-D Secure ACS Functionality.....	1
Summary of Required Actions	1
Cardholder Authentication Page.....	3
Challenge Generation.....	3
Reader Type.....	3
Unconnected.....	4
Connected.....	4
Perform Transaction Operation - Cardholder Authentication	4
Fallback.....	4
Display Details	5
Challenge Clarity.....	5
SecureCode™ Input Field	6
Verify SecureCode™	6
Rebuilding Input Data	6
Application Transaction Counter.....	7
Rebuilding the ATC.....	7
Updating ATC.....	7
Comparison of Reduced Cryptogram	7
Fraud Detection	8
Requirements and Recommendations	9
Requirements.....	9
Recommendations	9

Functional Requirements – Authentication Request Server
Introduction

Introduction

An Authentication Request Server services requests for authentication of cardholders equipped with MasterCard Authentication Application smartcards and a Personal Card Reader.

Authentication may be requested for a number of different reasons. The focus of this specification is authentication in the context of the MasterCard implementation of the 3D-Secure card-payment authentication scheme. However, the actual cardholder authentication itself is not specific to 3D-Secure and so the material in this chapter is deliberately presented in an authentication-neutral manner.

The various requirements and recommendations discussed here are summarized at the end of this chapter.

Responsibilities of an Authentication Request Server

- To maintain a database of enrolled cardholders & card details – In order to perform the actual authentication, a CAP Capable Authentication Request Server must hold all of the data that is necessary to verify SecureCodes™.
- To generate and send a Cardholder Authentication Page – Returned to the cardholder's browser in response to the action which prompted the start of the authentication request.
- To verify SecureCode™ – The SecureCode™ is 'returned' to the Authentication Request Server in the form of a HTTPS/POST containing the SecureCode™ in a textual numeric form.
- To maintain appropriate keys to regenerate application cryptograms in order to verify SecureCodes™ generated by the IOCs.

Modifications to Standard 3-D Secure ACS Functionality

3-D Secure Access Control Servers when written in a modular fashion should experience no change to 3-D Secure payment authentication transactions themselves, only in the actual cardholder authentication mechanism component of the ACS software which within the framework of 3-D Secure is proprietary to the card issuer.

Summary of Required Actions

Once the chip authentication process has been initiated, the Authentication Request Server must perform the following actions:

- Create a Challenge if one will be used in the authentication process.

Functional Requirements – Authentication Request Server

Introduction

- Generate the HTML Cardholder Authentication Page to deliver to the cardholder's browser. This page must;
 - Display the appropriate authentication transaction details and other authentication information to the cardholder.
 - If the PCR issued to the cardholder is dynamically determined to be an unconnected reader, then
 - display any Challenge, if appropriate
 - allow for an input field where the cardholder should enter the SecureCode™.
 - If the reader issued to the cardholder is dynamically determined to be a connected reader, then;
 - include the appropriate software component (typically ActiveX control) to communicate with the reader which should also allow for a fallback to an unconnected reader in the event of the reader not being able to operate in a connected mode
 - supply the software component with the appropriate input parameters so that it may instruct the PCR to perform an authentication operation
 - Display instructions to the cardholder detailing the actions they need to take for:
 - verifying the appropriate transaction details or other authentication reason
 - entering the Challenge into the reader, if one is used
 - inserting the correct card and entering their PIN on the Personal Card Reader
 - transferring the SecureCode™ from the Personal Card Reader back to the HTML Cardholder Authentication Page, if appropriate
 - if an unconnected reader is used, submitting the HTML form back to the Authentication Request Server, or canceling the authentication.
- Process the POSTed HTML form.
- Verify the SecureCode™ by
 - Rebuilding any missing input data for the application cryptogram generation
 - Generating an application cryptogram using locally stored keys
 - Comparing the locally generated cryptogram with the partial cryptogram received from the cardholder.
- Pass an indication of the authentication back to the process requiring the authentication and allowing it to continue in an appropriate manner.

Cardholder Authentication Page

Challenge Generation

An Authentication Request Server may have different requirements on whether a challenge is to be used, and if so, what form of challenge.

If a challenge is supplied to the PCR, then the SecureCode™ generated can be linked to a particular authentication request event.

If no challenge is supplied to the PCR, the inclusion of the card's ATC in the generation of the application cryptogram & subsequent partial supply in the SecureCode™ provides for some uniqueness, replay detection & temporal sequencing. However, without a challenge, an Authentication Request Server cannot be sure in what context the one-time passcode was generated, and that it was not previously captured and is now being used.

Where a challenge is to be used, there are no specific requirements as to what constitutes the input data for the challenge generation algorithm. The party generating the challenge is the same party that is verifying the response. i.e. the Authentication Request Server, and there is therefore no need to standardise on a common generation algorithm.

Issuers must define the algorithm & input data used for a challenge. For example it might be;

- a random number
- derived from a hash of transaction data
- based on the current date & time

However, this specification does have requirements on the format of any supplied challenge. A supplied challenge must be a decimal number of up to but no more than eight digits.



Personal card readers are required to accept up to 8 decimal digits, with or without leading zeroes, with the challenge being finally entered through an OK key on the reader.

Reader Type

The difference for an Authentication Request Server in whether a connected or unconnected reader is involved only concerns the method of communication with that reader.

Functional Requirements – Authentication Request Server

Cardholder Authentication Page



Note Before populating the SecureCode pop-up window with the issuer defined Cardholder Authentication Page, Authentication Request Servers that support both reader types may wish to determine whether a cardholder will be using a connected or an unconnected reader. Alternatively, the Authentication Request Server may wish to rely on the fallback mode to dynamically handle unconnected readers.

Unconnected

Unconnected readers require the cardholder to transfer any challenge to the reader by reading the challenge on the HTML Cardholder Authentication Page sent by the Authentication Request Server and typing in the challenge on the reader's keypad. The SecureCode™ is similarly transferred by reading the SecureCode™ displayed on the reader and typing it into the HTML form to be returned to the Authentication Request Server.

Connected

To communicate with a connected Personal Card Reader, it is necessary to use a software component that can be embedded in the HTML Cardholder Authentication Page and which is capable of making calls to the native operating system. On a Windows™ system, this is likely to be ActiveX component technology.

The component will need to be able to access standard smartcard-reader drivers and send an APDU command. On a Windows™ system, this means calling the PC/SC API.

Perform Transaction Operation - Cardholder Authentication

The embedded software component must send an APDU command to the PCR in order to instruct it to perform an authentication operation. Full details about the APDU command may be found in the Functional Requirements – Personal Card Reader chapter in the section Connectivity. However, the command is summarised below;

CLA = 80, INS = 12, P1 = 02, P2 = 01



Note Although special ‘authentication’ drivers/client software are not necessary, cardholders with connected readers must ensure that the appropriate standard drivers for their reader are installed on any computer on which they wish to use the reader.

Fallback

The embedded software component is intended to work with a connected reader. However, to cater for those times when it is not possible to work with a connected reader, the embedded software component must be able to fallback to an unconnected mode.

Functional Requirements – Authentication Request Server
Cardholder Authentication Page

The embedded software component should be able to detect most conditions where it is not possible to work with a connected reader:

- No operating system smartcard reader functionality available/installed
- No card readers available/installed
- When the **Personal Card Reader Confirmation** command APDU (CLA=80, INS=12, P1=00, P2=01) is sent, the expected valid response (sw1/2 = 0x9000, data = 0xD003‘PCR’) is not received within a reasonable timeout (500 ms for example).

Operating in fallback mode means presenting any required challenge to the cardholder and offering an input area in which the SecureCode™ of up to 8 numeric digits can be entered.³

Display Details

An Authentication Request Server requiring cardholder authentication for participation in a 3-D Secure transaction must follow the guidelines as defined in the [MasterCard SecureCode™ Enrollment and Implementation Guide] on what & how to display the transaction data. This sub-section defines extra display requirements pertinent to using the Chip Authentication Program.

Whilst the authentication scheme is aimed at cardholders who are active Internet users, and therefore familiar with using PC devices and the Internet itself, the scheme will also be used by an increasing number of novice users. Therefore, particular attention must be paid to ease of use and its applicability to novice computer users.

Challenge Clarity

The Challenge must be correctly entered by the cardholder into unconnected PCRs. The Challenge, where displayed, must be presented by the HTML Cardholder Authentication Page in a clear manner. It is recommended that the Challenge displayed on the page is on a ‘line’ of its own, larger and bolder than the explanatory text and in groups of up to 5 digits, as suggested below:

1
12
123
1234
12345
123 456

³ This might be done by either displaying this ‘fields’ in a dialog box, or enabling them to be visible on the Cardholder Authentication Page itself.

Functional Requirements – Authentication Request Server

Verify SecureCode(

123 456 7
1234 5678



Notes The challenge will not be displayed by a connected reader and need not be displayed on the HTML Cardholder Authentication page when a connected reader is used.

PCRs will not use any separators when the cardholder enters the challenge.

SecureCode™ Input Field

The HTML Cardholder Authentication Page generated for use with an unconnected reader must contain an input field into which the cardholder will enter the numeric SecureCode™ of up to 8 digits.

Following the optional Challenge entry, card insertion and PIN entry by the cardholder, the unconnected PCR will display the relevant SecureCode™ on its display. Since this display is very limited, the HTML Cardholder Authentication Page must also provide instructions to the cardholder regarding entry of the SecureCode™ into the SecureCode™ input field.

Verify SecureCode™

The HTML form data posted back from the Cardholder Authentication Page which was presented to the cardholder, contains the SecureCode™.

An Authentication Request Server must verify the SecureCode™, which can then be deemed as sufficient proof of cardholder presence & approval of the request presented to them.

Rebuilding Input Data

In order to verify the SecureCode™, the Authentication Request Server must compare the partial cryptogram received in the SecureCode™, with an equivalent cryptogram it must generate. To make this comparison meaningful, the cryptogram must be constructed using the **same input data** as used by the card at the time of authentication in real time, and within the time constraints required by the payments system.

The Authentication Request Server can easily re-construct the required input data using a combination of:

- assumed static values
- certain data transferred in the SecureCode™
- data retrieved from cardholder databases.

The IIPB is used by the PCR to determine which individual bits are to be transferred in the SecureCode™. For a given card, or technology, the IIPB must therefore be known or retrieved by the Authentication Request Server in order to rebuild this data.

Functional Requirements – Authentication Request Server
Verify SecureCode(

Application Transaction Counter

The authentication application on the smartcard generates the Application Cryptogram (AC) using the Application Transaction Counter (ATC) as one of its inputs. The ATC is incremented by the card itself as part of the transaction process involved in generating the AC and once the ATC has reached its maximum value of 65535, the card is no longer valid. This means that the ATC will always be a unique value, resulting in a unique AC always being generated. ATCs therefore avoid replay of Application Cryptograms.

Rebuilding the ATC

The application transaction counter should be rebuilt where only a partial counter has been sent. The last known value for the ATC should be retrieved, adjusted for rollover, and used in the authentication validation.

Where a partial ATC is reconstructed, the reconstruction algorithm requires that if the received partial ATC is less than or equal to its known equivalent, it should be assumed that a rollover occurred. In this case, the higher bits should be incremented appropriately. This means that a reconstructed ATC will never be less than or equal to the known ATC. If a replayed transaction is used, it will therefore be rejected by virtue of the ATC reconstruction algorithm arriving at an increased and thus invalid ATC for the associated AC.



A card which has been used to produce multiple unsubmitted authentications and has 'over-incremented' its ATC can only again be used for authentication transactions if and when its ATC is re-synchronised with the Authentication Request Server's ATC record.

Updating ATC

Once the authentication validation, using the reconstructed ATC, has proved successful, the last known ATC should be updated with the reconstructed ATC. This way, the risk of replay attacks, where the same SecureCode™ is re-used repeatedly, is omitted.

Comparison of Reduced Cryptogram

The cryptogram produced by the card is a MAC of 8 bytes in length. The limited bandwidth of the link between the unconnected PCR and the HTML Cardholder Authentication Page means that as part of the data reduction, not all of these 8 bytes are transferred in the UCAF.

Changes will also be needed to the 'security box' that regenerates the ICC cryptograms. The comparison processes will need to be adapted to support the reduced length cryptogram.

Functional Requirements – Authentication Request Server
Verify SecureCode(

Fraud Detection

Because the size of the Application Cryptogram transferred in the SecureCode™ is small, and the Challenge data does not necessarily vary for each transaction, fraud detection systems should be used at the issuer level.

**Functional Requirements – Authentication Request Server
Requirements and Recommendations**

Requirements and Recommendations

Requirements

The following table lists the requirements that apply to Authentication Request Servers:

Function	Requirements
User Interface Challenge Display	When using an unconnected reader, the Challenge must be displayed in a clear manner, and in a larger typeface than the transaction details.
SecureCode™ Entry	<ul style="list-style-type: none"> • When using an unconnected reader, the input area accepting the SecureCode™, typed in by the cardholder, should display entered digits in the same style of typeface in which the challenge is/would be displayed. <p>SecureCodes™ are defined as numeric values of up to 8 digits.</p>
SecureCode™ Card Database – Validation	Due to the reduced data that is transferred in the SecureCode™, the systems for decoding and verifying the SecureCode™ may need access to a card database in order to retrieve any card specific static data.
Reduced Cryptogram	Cryptographic systems must be upgraded where necessary to support the comparison of the reduced cryptogram passed in the SecureCode™.
Application Transaction Counter	The ATC must be rebuilt according to the data transferred in the SecureCode™ and the data held in the card database. The ATC held in the card database must only be updated on successful verification of the Application Cryptogram.

Recommendations

The following table summarizes the recommendations that apply to Authentication Request Servers:

Function	Recommendations
Issuer Host Processing	Fraud Detection – Because the size of the Application Cryptogram is small fraud detection systems should be used at the issuer level.

Functional Requirements – Personal Card Reader
Requirements and Recommendations

3

Functional Requirements – Personal Card Reader

This chapter describes the functional requirements that apply to the Personal Card Reader for the purposes of authenticating transactions using the Chip Authentication Application.

Functional Requirements – Personal Card Reader

Introduction	1
Reference Specification.....	1
Overview	2
PCR – Processing and Data Flows	2
Unconnected Reader	3
Connected Reader.....	5
Issuer Internet Proprietary Bitmap (IIPB)	6
Length of IIPB	7
Effective IIPB Length.....	8
When to Check for a Valid IIPB.....	8
IIPB Error Indication.....	8
Requesting an Application Cryptogram	9
Using Unpredictable Number in GENERATE AC.....	9
Processing the GENERATE AC Response	9
IIPB Data Token.....	10
Transferring the IIPB Data Token in the SecureCode.....	10
SecureCode.....	11
Creating the SecureCode	11
Format of SecureCode.....	11
Connected Personal Card Reader.....	11
Cardholder Interaction	12
Cardholder Data Entry.....	12
Cardholder Cancellation.....	12
Challenge	12
Completion and Editing of Challenge Entry	12
No Challenge Entry.....	12
PIN Entry.....	13
Handling of Incorrect PIN Entry.....	13
Blocked PIN.....	13
SecureCode Display.....	13
Connectivity.....	15
Dual Mode	15
APDU Command	15
Perform Transaction Operation.....	15

Functional Requirements – Personal Card Reader

Command	15
Parameters	16
Current Transaction Operations	16
Data.....	17
Response.....	18
Personal Card Reader Confirmation	19
Cardholder Authentication	20
Firewall.....	21
 Application Commands and Processing.....	22
Card Activation	23
Application Selection.....	25
Initiate Application Processing	26
Read Application Data	26
Offline Card Authentication	27
Process Restrictions	27
Cardholder Verification	28
Terminal Risk Management	29
Terminal Action Analysis	29
First Action Analysis	29
Terminal Online Processing.....	31
Issuer to Card Script Processing.....	31
Transaction Completion	31
SecureCode Generation	32
Exception Handling.....	33
 Requirements and Recommendations.....	34
Requirements	34
Recommendations	36

Functional Requirements – Personal Card Reader
Introduction

Introduction

The **Personal Card Reader (PCR)** is the key component in the Chip Authentication Program. This chapter defines the functional requirements for the PCR within the context of CAP and provides:

- an overview of the data and processing flows as they concern the PCR
- a description of the new card data object, the IIPB, that has been introduced specifically for cardholder authentication to allow for a more generic PCR implementation
- the interactions with cardholders
- the EMV commands and the processing actions that the card reader must take
- a summary of requirements and recommendation that apply to the PCR.

This chapter makes repeated references to the **[Proceed]** and **[Cancel]** keys on the keypad of the PCR. Depending on the actual keypad used:

- The **[Proceed]** key may be marked **OK** or **Approve** – the purpose being to indicate confirmation, or normal completion, of the current action.
- The **[Cancel]** key may be marked **Stop** or **Abort** – the purpose being to indicate cancellation, or abnormal termination, of the current action.

Reference Specification

The reference specifications used for the behavior between the card and terminal in the transaction are:

- M/Chip—Terminal Requirements for Debit and Credit; Version 4.0, October 2001.
- M/Chip - Functional Architecture for Debit and Credit; Version 1.0, January 2003.
- MasterCard Recommended Specifications for Debit and Credit on Chip; Version 2.1, October 1999.
- MasterCard Chip Personalization Specifications for Debit and Credit on Chip; Version 2.2, October 1999
- M/Chip Lite; July 2000.
- M/Chip 4 Card Application Specifications for Debit and Credit; Version 1, October 2002.
- M/Chip 4 Member Guide to Debit and Credit Parameter Management; (to be published).

Functional Requirements – Personal Card Reader Overview

Overview

PCR – Processing and Data Flows

The following overview is in the form of scenarios for both an unconnected and connected Personal Card Reader.

The main difference between a connected PCR and an unconnected PCR is user convenience. In case of a connected PCR the link between the PC and the PCR is used to carry data to and from the PCR; in case of an unconnected PCR this data must be 'copied' by the Cardholder.

Where data is keyed into the PCR, this scenario gives an illustration of that data entry by displaying each digit entered in **bold**, with the most recently keyed digit, in **bold underline**.

Prompts are shown only as a guide to implementation and do not constitute requirements for display, as implementers are expected to use appropriate prompts in appropriate locales.

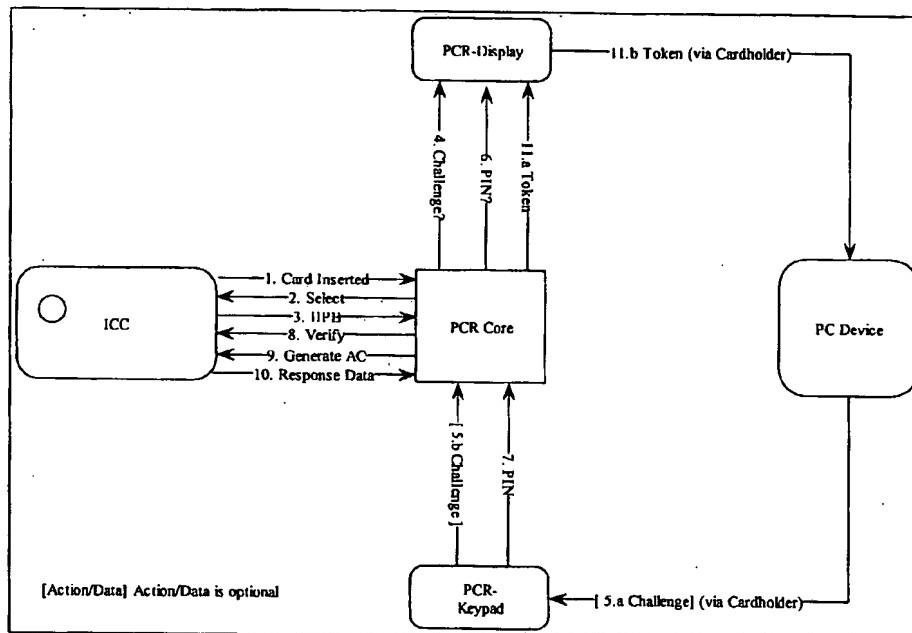
Figure 1.3 & Figure 1.4 show conceptual diagrams to illustrate the scenario text. They are not detailed illustrations of the commands sent to the card or the exact processing steps required at the Personal Card Reader. Only those elements which help illustrate the system, its data structures and general processing are shown.

The numbers in each diagram are referenced in the text that follows it.

Functional Requirements – Personal Card Reader
Overview

Unconnected Reader

Figure 1.3—PCR Scenario – Data Flows



1. The cardholder is requested by the reader to insert their card. The cardholder inserts their MasterCard Authentication enabled card into the personal card reader.

Insert Card



Note With unconnected readers, the action of inserting the card might turn the reader's power on, or the cardholder may need to press a power button to turn it on.

2. The PCR looks for a MasterCard authentication application on the card and selects it.
3. The PCR reads selected data elements from the IOC.
4. The PCR prompts the cardholder to enter a Challenge.

The generation of the Challenge is proprietary to the Card Issuer; it will be used for the Unpredictable Number (UN) in the EMV Transaction handling.

Challenge>

5. The cardholder must enter this Challenge on the keypad of the PCR and press the [Proceed] key to indicate completion of Challenge entry.

5

58

581

Functional Requirements – Personal Card Reader Overview

5811

58113

581139

5811396

58113967

[Proceed]



Where Authentication Request Servers do not require a challenge, the cardholder may simply press the [Proceed] button without entering any challenge digits. Whereupon the PCR will use a value of 0 for the UN in the later GenerateAC command.

6. The PCR displays a prompt for the cardholder to enter their PIN:
Enter PIN
 7. The cardholder enters their PIN digits, and presses the **[Proceed]** key to indicate completion of PIN entry, as illustrated with the 5-digit PIN example below:

—
—
—
—
—

[Proceed]

8. The PCR submits the PIN to the IOC for verification.

Error Check: If the ICC reports an invalid PIN entry, the PCR informs the cardholder of the number of PIN attempts remaining:

Bad PIN, 2 left

The cardholder then enters the correct PIN, presses the [Proceed] key, and the PCR reports a valid PIN entry.

☆☆☆☆☆

[Proceed]

PIN OK!

9. The device prepares a **GENERATE AC** command, using the challenge data for the Unpredictable Number⁴, a valid TVR and all other data requested by the Card Application set to '0' (indicating the information is not available) The PCR sends the command to the ICC.
 10. The ICC replies with a **GENERATE AC** response. The PCR uses the IIPB read from the card to determine the bits from the response to the **GENERATE AC** that must be stripped and compressed into the IIPB Data Token.

Error Check: If the length of the IIPB does not match the length of the data elements returned by the IOC in response to the Generate AC (length of the concatenated fields CID, ATC, AC and IAD), the PCR displays the message:

4 If no challenge was entered, the reader will use a value of 0 for the UN.

**Functional Requirements – Personal Card Reader
Overview**

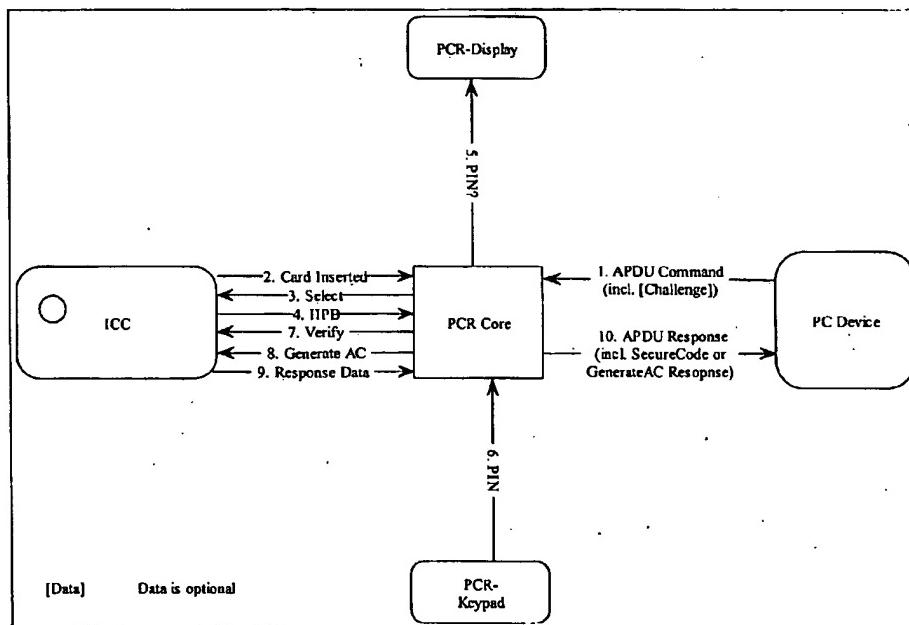
Error

11. The, unconnected, PCR then computes and displays an 8-digit SecureCode.

10348247

Connected Reader

Figure 1.4—PCR Scenario – Data Flows



A connected reader differs in;

- it's method of starting the transaction. The receipt of the appropriate APDU command starts the transaction rather than the insertion of a card or the powering on of the reader.
- it's method of receiving any challenge data. The cardholder is not asked to enter a challenge, as any challenge data is supplied with the APDU that initiated the transaction.
- it's method of returning the SecureCode™. The SecureCode, which must be calculated in the same manner as when working in an unconnected mode, is required to be returned in the APDU response. This ensures that the Authentication Request Server can treat connected & unconnected readers in the same manner when processing the response.

Functional Requirements – Personal Card Reader
 Issuer Internet Proprietary Bitmap (IIPB)

Issuer Internet Proprietary Bitmap (IIPB)

The Issuer Internet Proprietary Bitmap (IIPB) is a data object with a tag of '0x9F56', introduced as part of the Chip Authentication Programme, whose presence on a card is required. It is defined by the issuer and used by the PCR to determine which bits of the ICC's **GENERATE AC** response must be used when generating authentication data.

When an unconnected card reader is used, the amount of data that can be realistically transfer back to the PC device by a cardholder is limited. The PCR can therefore only transfer a selected portion of the data required by the issuer to re-compute the AC, and hence validate the SecureCode.

The response, by the ICC, to the first **GENERATE AC** command is made up of the following data elements:

- Cryptogram Information Data (CID)
- Application Transaction Counter (ATC)
- Cryptogram computed by the ICC (AC)
- Issuer Application Data (IAD).

These data elements contain data that is either:

- **Unique to this transaction** and must be transferred from the PCR to the Interface Application.
- **Obtainable from other sources** and therefore does **not** need to be included in the SecureCode. Such data will be:
 - assumed to have particular values for the issuer's given card scheme
 - unique to the ICC and known (or at least deducible) by the issuer host, via its card database.

The issuer defines the IIPB in the form of a bit-mask, to be used by the PCR to select only those bits from the **GENERATE AC** response that the issuer requires to verify the cryptogram. The number of bits marked as 'required' determines the size of the SecureCode produced by the PCR and must not exceed 26 bits. 26 bits is the maximum number of bits that can be transferred with an 8-digit decimal number. (67,108,863)

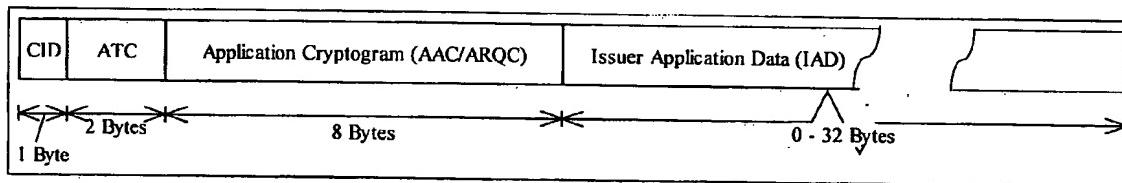
Functional Requirements – Personal Card Reader
Issuer Internet Proprietary Bitmap (IIPB)

Figure 1.5 shows the structure of the IIPB. The bits that make up the IIPB are considered as transmit flags, indicating which bits from the **GENERATE AC** response are required by the issuer for inclusion in the SecureCode. These flags correspond on a bit-for-bit basis to the bits that must be sent from the:

- CID 1 byte
- ATC 2 bytes
- AC 8 bytes
- IAD 0 – 32 bytes.

Therefore, the IIPB can vary in length from 11 bytes, where no IAD is defined (unlikely) to 43 bytes where an issuer's application technology uses the full 32 bytes available to the Issuer Application Data (IAD).

Figure 1.5— IIPB Structure



The IIPB is used as a bit-mask which allows the PCR to derive an 'IIPB Data Token' which, when 'compressed', forms the SecureCode passed to the authentication requester.

An IIPB allows the **issuer** to determine and be completely selective as to the data needed to validate the SecureCodes used in the Chip Authentication Program.

Length of IIPB

The IIPB is used as a mask against the concatenation of the data elements CID, ATC, AC and IAD, resulting in a structure between 11 and 43 bytes in length. The PCR must determine that the length of the IIPB matches the length of the data items returned in the card's GenerateAC response.



Note It is not necessarily a straight mask on the response data, since both Format 1 (untagged) and Format 2 (tagged) GENERATE AC responses must be handled by the PCR. Format 2 response data includes the tags and lengths as well as the values of CID, ATC, AC and IAD.

Functional Requirements – Personal Card Reader
Issuer Internet Proprietary Bitmap (IIPB)

Effective IIPB Length

The ‘effective IIPB length’ refers to the number of bits – as defined by the IIPB – to be transferred within the IIPB Data Token (this is governed by the number of bits in the IIPB itself that are set to 1 to indicate transfer required).

The effective IIPB length cannot exceed 26 bits, as this would require more than 8 digits for the token.

When to Check for a Valid IIPB

The Issuer Application Data (IAD) may be between 0 and 32 bytes. The length of the IAD will not be known to the PCR until it is returned from the ICC in the response to the **GENERATE_AC** command.

Therefore the check for IIPB length cannot be done until the **GENERATE_AC** response is received by the PCR.

IIPB Error Indication

If the IIPB length does not match or has defined too many bits for an unconnected device, the PCR must stop processing and display an error indication, e.g.

Error

Requesting an Application Cryptogram

The Chip Authentication Program uses an Application Cryptogram (AC) as the mechanism for authenticating the ICC and the cardholder.

The EMV command **GENERATE AC** is used to request the IOC to generate an Application Request Cryptogram (ARQC)

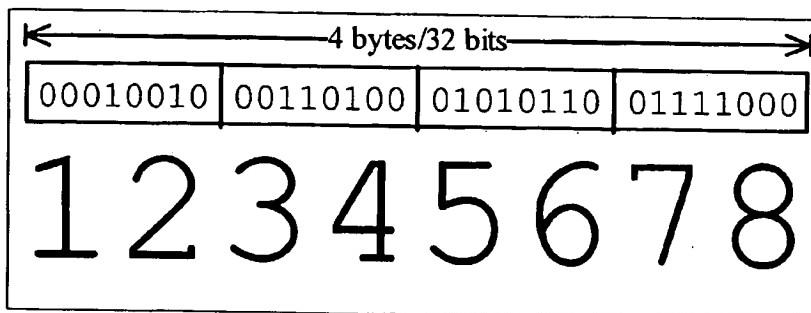
- The data that must be supplied in this command is specified by the EMV data element known as CDOL1; details on the contents of the CDOL1 for the different Card Application specifications are included with their respective personalisation details.

Using Unpredictable Number in GENERATE AC

The Unpredictable Number (UN) is a 4-byte/32-bit component of the data passed to the ICC in the **GENERATE AC** command. It is a number (or data) that is unpredictable to the IOC, as opposed to the application.

The challenge passed to the PCR is used as the 'UN' for cryptogram generation. The maximum number of 8 digits for the Challenge are used in a BCD (Binary Coded Decimal) form when sent to the card. Any challenge of less than 8 digits should use leading zero padding up to 8 digits when creating the UN.

Figure 1.6— Illustration of 8 digit Challenge as BCD



Processing the GENERATE AC Response

This section describes how the PCR must process the response from the IOC to the **GENERATE AC** command in order to arrive at the SecureCode that must be returned to the Interface Application.

Functional Requirements – Personal Card Reader
Requesting an Application Cryptogram

IIPB Data Token

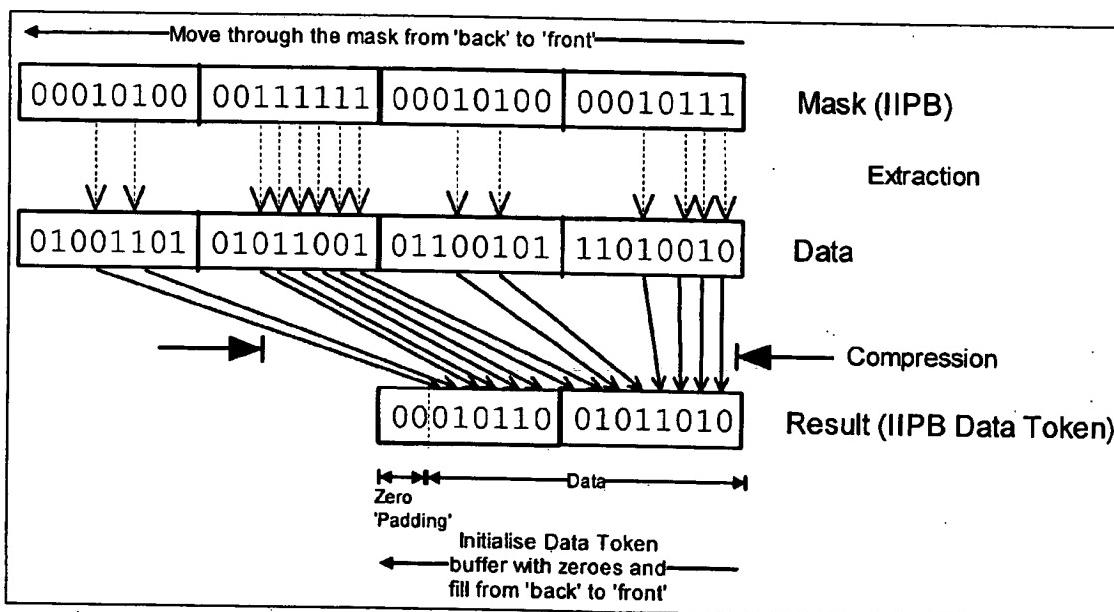
When using an Unconnected Personal Card Reader (and at the option of the Authentication Request Server also for Connected Readers), the full response to the **GENERATE AC** command is too large to be sent to the issuer. The PCR uses the Issuer Internet Proprietary Bitmap (IIPB) to perform a data extraction and compression process.

A bit setting of '1' in the IIPB indicates the corresponding bit position in the response data is 'required' and needs to be sent.

A bit setting of '0' indicates that the issuer either knows, or is able to otherwise derive, what the bit setting should be and thus the bit does not need to be sent as part of the SecureCode.

The IIPB Data Token is built up, from right to left, with the first bit to be extracted placed into bit 1 of the last byte of output data, the second in bit 2, etc. The IIPB Data Token is filled in this manner until there are no more bits to transfer, as shown in Figure 1.7:

Figure 1.7— Bit Extraction and Compression



Transferring the IIPB Data Token in the SecureCode

The IIPB Data Token is the data that is transferred from the PCR to the Interface Application. Connected readers can transfer this data directly to the Interface Application, whereas for unconnected readers, the cardholder must transfer this data manually.

Functional Requirements – Personal Card Reader
Requesting an Application Cryptogram

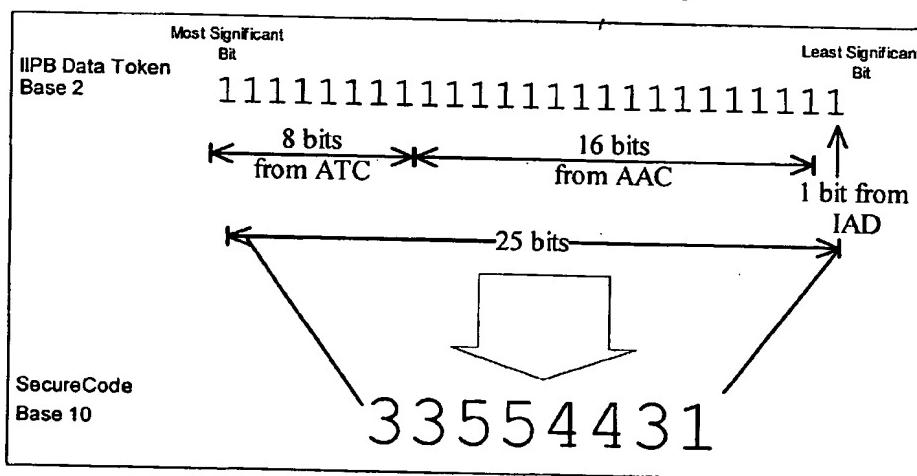
SecureCode

Personal Card Readers must compute a number that represents the bit pattern of the data to be transferred. An unconnected reader will then display this number – the SecureCode – so that the cardholder can enter it into the appropriate field displayed by the Cardholder Authentication Page.

Creating the SecureCode

It is important that the algorithm used for converting the required bits into displayed numeric digits is interoperable and thus reversible on the Authentication Request Server. The same algorithm used to convert from bits to token must be reversed to convert from token to bits. The most ‘compressed’ way to do this is to treat the bit pattern as a binary number and perform a mathematical conversion from Base-2 to Base-10, as shown below.

Figure 1.8—Example of Conversion of Required Data Bits from Base2 to a Base10 Token based on M-Chip/Lite 2.1 IIPB Encoding



Format of SecureCode

The SecureCode must be no more than 8 numeric digits (hence a maximum IIPB Effective Length of 26 bits) which represent the IIPB Data to transfer.

Connected Personal Card Reader

For readers working in connected mode, the SecureCode is computed in the same way as for unconnected mode, but is not displayed to the cardholder. It is transferred directly to the Interface Application in the APDU response to the **PerformTransactionOperation-CardholderAuthentication** command that triggered the authentication transaction.

Functional Requirements – Personal Card Reader
Cardholder Interaction

Cardholder Interaction

Cardholder Data Entry

The following points relate to the entry by the cardholder of the following data:

- Challenge – Unconnected readers only
- PIN – Both connected & unconnected readers

Cardholder Cancellation

The cardholder must be able to cancel/stop the authentication process at any time where data entry is requested by pressing the [Cancel] key, removing the card or, if offered by the PCR, powering off the reader.

Challenge

An unconnected PCR must only allow Challenge entry when a valid IOC is inserted in the PCR. The Challenge must be the first piece of data requested by the PCR for a given transaction.

Completion and Editing of Challenge Entry

The PCR must allow the cardholder to 'backspace' and erase an entered digit prior to indicating the completion of data entry.

The cardholder must indicate completion of the Challenge entry by pressing the [Proceed] key.

The Challenge will be of a variable length, with a maximum length of 8 digits. The PCR must be able to accept shorter challenges – challenges with UN values from 0 upwards (where no leading zeros are used).

No Challenge Entry

If no challenge was supplied by the authentication requester, then the cardholder will simply press the [Proceed] button to skip challenge entry, causing the reader to use the default value of 0 for the UN in the GenerateAC.



An unconnected reader has no way of knowing whether it is indeed valid for the cardholder to skip the challenge entry, as they might just have decided they did not want to enter the challenge. However, in such cases, the SecureCode will not correctly validate, as the input would not be as the authentication requester was expecting. The non-entry of a challenge is, therefore, purely an issue for the validation of the SecureCode.

Functional Requirements – Personal Card Reader
Cardholder Interaction

PIN Entry

The cardholder must enter their PIN on the PCR. During PIN entry:

- The PCR must provide visual feedback to the cardholder by displaying a '*' character for each PIN digit entered. This visual feedback must build up from right to left, as digits are entered.
- There must be no digit entry indicators used, such as dots or dashes, that indicate digits still to be entered.
- The PCR must not provide any audible feedback that would indicate which keys were used for PIN entry.
- The PCR must allow the cardholder to 'backspace' and erase an entered digit prior to indicating completion of PIN entry.
- The PCR must allow for PIN lengths of between 4 and 12 digits.
- The [Proceed] key must be used to indicate completion of PIN entry.

Handling of Incorrect PIN Entry

Following incorrect PIN entry, the PCR must communicate to the cardholder that the PIN entered was invalid. The PCR must display an indication of the number of PIN attempts remaining, together with a prompt for the cardholder to re-enter their PIN.

The PCR should only allow a maximum of three PIN retries, even if the card might allow more.

When there are no PIN tries remaining:

- the PCR must **abort** the transaction
- a **GENERATE AC** command, requesting an AAC, must **not** be sent to the card, as might be the case with a conventional terminal.

Blocked PIN

Before asking for **any** cardholder input, it is recommended that the PCR check the status of the card. If there are no PIN tries remaining, the application is 'blocked' and the authentication cannot proceed. If so, the PCR should inform the cardholder that the application is blocked and abort the authentication process.

SecureCode Display

Unconnected readers must display the SecureCode for at least 30 seconds in order to allow a cardholder reasonable time to transfer the SecureCode to the Cardholder Authentication Page.

Functional Requirements – Personal Card Reader
Cardholder Interaction

The SecureCode must only be displayed while the card is physically inserted into the reader.
The SecureCode must be removed from the display if the card is removed, or if the
cardholder presses the [Cancel] key.

Functional Requirements – Personal Card Reader
Connectivity

Connectivity

Some cardholders may be equipped with card readers able to operate in ‘connected’ mode. When a cardholder uses a connected PCR they need only enter their PIN on the card reader to complete an authentication. All of the required transaction and authentication data is transferred automatically between a software component running on the cardholder’s PC Device and the connected PCR:

- any Challenge required by the authenticating requestor (as entered by the cardholder into an unconnected PCR)
- any amount and currency that the cardholder is required to confirm prior to PIN entry.
- the SecureCode generated by the PCR (as entered by the cardholder into the Interface Application when using an unconnected PCR).

The PCR always behaves as an autonomous terminal, regardless of the connection mode.

Dual Mode

Connected readers must be equipped with a connection cable that may be removed from the reader itself and be capable of working in either a connected or an unconnected mode.

APDU Command

An authentication transaction is initiated on a connected PCR by means of a specific APDU command, designed to be interpreted **only** by the reader and **not** sent on to the card. The data sent with the APDU command carries the input data required to perform a CAP authentication transaction. The response to this command carries the SecureCode.

The advantage of using this technique is that only standard drivers are required for the card reader. Any driver capable of sending an APDU to an ICC is also able to send the **PerformAuthenticationOperation** command.

Perform Transaction Operation

Command

The **PerformAuthenticationOperation** command is in fact a more generic **PerformTransactionOperation** command, with a parameter value that indicates that an ‘authentication’ operation is to be performed. This approach supports any future commands defined by MasterCard which are intended for the reader and not the ICC. Such commands can use the same APDU command values, but with different parameters.

Functional Requirements – Personal Card Reader

Connectivity

The particular **CLA**, **INS** combination selected for this command respects standard ISO conventions:

- The class byte value of '80' means that the command does not use secure messaging, and the format of the command follows the conventional data structure:

CLA, INS, P1, P2, Lc, Data, Le⁵

- The instruction byte value of '12' means 'Perform Transaction Operation'.

The PCR will both intercept and interpret the command. Therefore, although the IOC may have its own different interpretation of the 'Perform Transaction Operation' command, this is not an issue as there is no possibility that this command will be passed to the IOC (see also the Firewall section later in this chapter).

Parameters

The different operations to be performed will be identified according to the **P1** parameter value. A **P1** value of **0x02** indicates 'Cardholder Authentication'⁶.

Different formats of the data required to perform Cardholder Authentication, and the expected response data format, are indicated by the **P2** parameter.

e.g. A **P2** value of **0x01** indicates that a SecureCode is required in the response whilst a value of **0x02** indicates the full response to the GenerateAC command should be returned.

If a PCR does not recognize the **P1** value sent in a **PerformTransaction Operation** command, it shall reply with a status word response of:

sw1sw2 = 0x6A86

meaning 'Invalid P1 value (Unknown transaction)'.

Current Transaction Operations

P1	Meaning
'00'	Personal Card Reader Confirmation. Defined in this specification.
'01'	Value reserved by MasterCard for use with the Chip-UCAF service.
'02'	Cardholder Authentication. Authentication using an authentication AID. Defined in this specification.

⁵ Will always be '00' indicating the reader should return all of the data it is trying to.

⁶ A value of **0x01** indicates Payment Authentication – introduced to support Chip-UCAF, which uses a payment application AID and different default values. See the references section for where to read more about UCAF authentication.

Functional Requirements – Personal Card Reader
Connectivity

Data

The data required to perform the particular transaction operation must be supplied in the APDU command data area, in 'TLV' format. To reduce the TLV decoding requirements for readers, the following requirements will apply to data sent in this format:

- Standard tags will be used where available and custom tags will be defined for new data items (e.g. SecureCode™).
- Since the total data space available in an APDU is limited, no data item will exceed 127 bytes in length, and therefore all lengths will be encoded using 1 byte only.
- For a given value of P2, data elements that are present will always appear in the same order – optional data elements are supported (e.g. amount).
- For increasing values of P2 for a given value of P1, the data format (i.e. order of data elements) will always be backwards-compatible as new data elements will appear on the end.

The effect of these requirements is that:

- a connected PCR supporting a particular version of this specification need not implement a TLV parser
- connected PCRs that wish to be more flexible about support of future commands need only implement a very basic TLV parser.

Functional Requirements – Personal Card Reader
Connectivity

Response

Any data returned with a successful transaction response will be TLV encoded.

The following are standard status word values which are specified for the implementation of the **PerformTransactionOperation** command by PCRs, irrespective of the particular transaction (P1 value) to perform. Individual transaction operations may define additional status word values to indicate situations specific to those operations:

Status Word	Meaning
sw1sw2	
0x9000	Transaction completed successfully. Individual transaction operations may define specific data that is returned in addition to the status word. Any returned data will be defined by each individual transaction operation. Just as the specification of the input data is governed by the value of P2, the specification of any response data is also governed by the same value.
0x6283	Application is blocked. The response must be returned before displaying any error prompts.
0x6700	Wrong length: Lc ≠ Sum(L(Parameters)). The response must be returned before displaying any error prompts.
0x6987	Expected data object(s) missing, unable to continue with the transaction. To be used whenever a mandatory data object is not supplied.
0x69F0	Transaction operation stopped by cardholder. Transaction terminated. The response must be returned before displaying any error prompts.
0x69F1	Transaction operation stopped by reader. Transaction terminated. The response must be returned before displaying any error prompts.
0x6A86	Invalid P1 value (i.e. unknown transaction).
0x6C00	No PIN tries remaining. The response must be returned before displaying any error prompts.
0x6F00	Unknown error. The response must be returned before displaying any error prompts.

Functional Requirements – Personal Card Reader
Connectivity

Personal Card Reader Confirmation

Command format: **CLA = 80, INS = 12, P1 = 00**

The following table shows the required Data, which must be encoded in TLV Format:

P2 = 01	Description
Data Object/Presence	
No data sent	The command is to determine if a connected smartcard reader is a Personal Card Reader, as defined by this and other MasterCard specifications, or not.
Response Status	• sw1sw2 = 0x9000 – Transaction completed successfully.
Mandatory	
Confirmation String • Tag – 0xD0	
Mandatory	Length – 0x03 Value – "PCR"

Functional Requirements – Personal Card Reader
Connectivity

Cardholder Authentication

Command format: CLA = 80, INS = 12, P1 = 02

The following tables show the required Data, which must be encoded in TLV Format:

P2 = 01	Description
Data Object/Presence	
Challenge Optional	<ul style="list-style-type: none"> • Tag – 0x9F37 • Length – 4 • Value – Challenge as would be displayed to and entered by a cardholder, in BCD format with leading zero padding to 8 BCD digits/4 bytes. This value can be passed straight to the card as the Unpredictable Number. <p>Default Action – If no value is supplied, a default value of zero should be used for the Unpredictable Number in the GENERATE AC command.</p>
Response Status Mandatory	<ul style="list-style-type: none"> • sw1sw2 = 0x9000 – Transaction completed successfully.
SecureCode Mandatory	<ul style="list-style-type: none"> • Tag – 0xC1 • Length – Appropriate • Value – SecureCode™ that would be displayed on the screen when in unconnected mode, encoded into BCD format with leading zero padding to a complete byte where required (e.g. 7 digit SecureCode™ would be 6 digits of BCD).

Functional Requirements – Personal Card Reader
Connectivity

Firewall

In order to protect the integrity of MasterCard cards inserted into a Personal Card Reader, all PCRs are required to prevent APDU commands sent by the PC device from reaching an inserted MasterCard card. For any command not recognized as being 'allowed', the PCR must respond with:

sw1sw2 = 0x6982

to indicate: "Command not allowed – Security status not satisfied".

Although, according to this specification, the only command that a PCR will recognize is **PerformTransactionOperation**, it is possible that other MasterCard specifications have other requirements that might require Cardholder Authentication functionality. Even so, there will continue to be requirements intended to address the protection of the integrity of MasterCard cards inserted into any such reader.

Notes

This specification or its replacement determines the behavior and requirements for any MasterCard specified 'intelligent reader' that is required to implement Cardholder Authentication functionality, defined by CLA=80, INS=12, P1=02 in addition to any additional functionality.

Readers that perform other functionality, but do also include Cardholder Authentication, must ensure that the other functionality does not affect the integrity nor operation of the Cardholder Authentication operation; this requirement will be validated by the MasterCard Type Approval process.

Functional Requirements – Personal Card Reader
Application Commands and Processing

Application Commands and Processing

This section defines the EMV card processing steps that the PCR must perform in order to obtain an Application Cryptogram. Technically, the PCR will behave as a standard unattended personal POS terminal.

Figure 1.9 shows the steps involved in a standard EMV transaction. Due to the low cost and specific nature of the PCR, requiring the card simply to generate an ARQC or an AAC, many of the standard EMV processing steps can be simplified or even skipped. The type approval process for PCRs will take this reduced EMV functionality into account.

This simplicity is particularly important where card issuers are comfortable that their cardholders will use a specific implementation of PCR and that the ICC application used will be sufficiently in step with the terminal application running within the PCR.

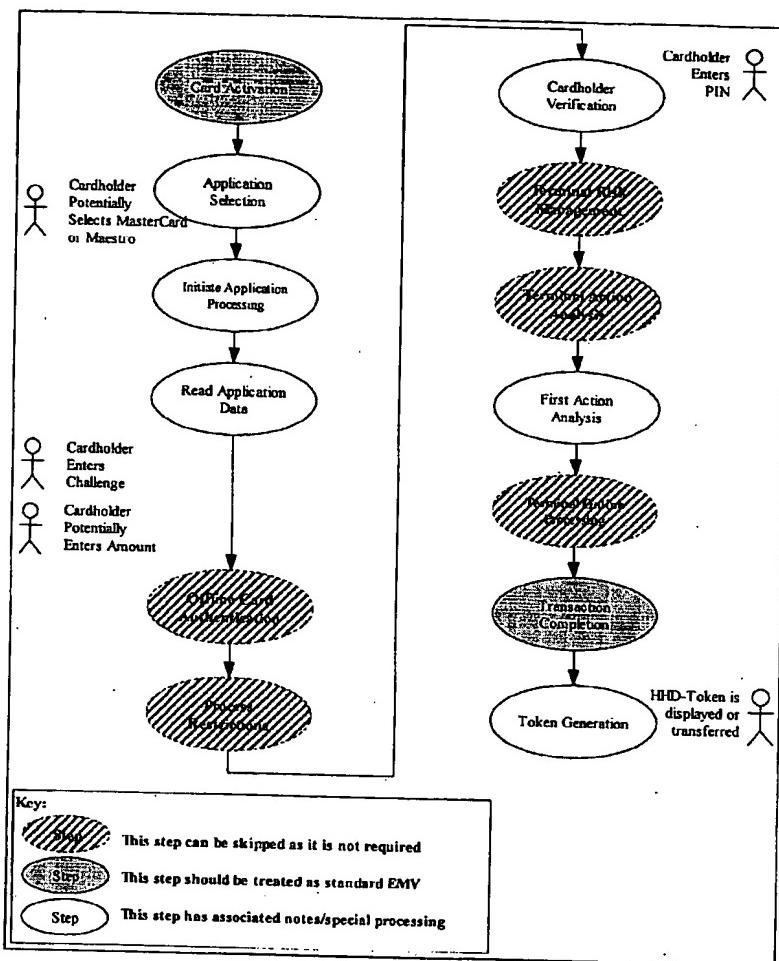
The text following the diagram, describes each of the steps shown. The steps that may be skipped by all PCRs are further identified in their description. Furthermore, those steps that may be optimized for a specific card implementation are also identified.

In the following text:

- The conventional names for EMV commands are shown in this description in the following font: **EMV COMMAND**.
- The letters **T** and **C** are used to distinguish between the Terminal (**T**) and Card (**C**) aspects of the processing.

Functional Requirements – Personal Card Reader
Application Commands and Processing

Figure 1.9—ICC Transaction Flow



Card Activation

The cardholder must insert the card into the PCR when authenticating a transaction.

All cards must be 'EMV Level 1' compliant. MasterCard does not impose support for a particular transmission protocol, therefore the PCR will need to support both the character protocol ($T=0$) and the block protocol ($T=1$) for communication between card and PCR. Where the character protocol ($T=0$) is used, the PCR should support both the direct convention (TS='3B') and the inverse convention (TS='3F').

T Terminal Processing:

60475639 . 060403

Functional Requirements – Personal Card Reader
Application Commands and Processing

The terminal RESETs the card.

Functional Requirements – Personal Card Reader
Application Commands and Processing

C Card Processing:

The card returns an **ANSWER TO RESET** (ATR) which may contain proprietary data.

T Terminal Processing:

Any data returned in the ATR is out of scope of the EMV specifications and should be ignored by the terminal.

If the card is removed at any time after the transaction has started, the transaction must be aborted and no SecureCode displayed.

Application Selection

This manual describes the interoperable application selection process as specified in EMV.

The application selection process is the process by which the terminal uses data from the ICC to determine which ICC application to use to produce an application cryptogram. The process consists of two steps:

1. Create a list of ICC applications that are supported by the terminal.
2. Select an application from the list generated.

A complete description of the EMV Application Selection process can be found in EMV 2000 Terminal Specification – Application Selection.

T Terminal Processing:

The terminal issues a **SELECT** command to select the following Application Identifier:

- Application Id=0x0xA000000048002

C Card Processing:

The ICC initializes the proper application context and returns data that is specified for the selected application, including:

- Information used for the dialogue between the PCR and the cardholder such as the application label assigned by MasterCard (i.e. "MasterCard" or "Maestro").
- The Processing Options Data Object List / PDOL identifying the data requested by the ICC Application to set its transaction context.

T Terminal Processing:

The terminal must check that the command completion code returned by the ICC does not indicate that the application is blocked for normal transaction handling (**sw1sw2 = 6283**). If the application is not blocked, the terminal stores the data returned by the ICC

Functional Requirements – Personal Card Reader

Application Commands and Processing

for later use. If the application is blocked the terminal must display a message to the cardholder and stop processing.

Terminal applications must be prepared to receive additional data.

Initiate Application Processing

The terminal initiates transaction processing.

T Terminal Processing:

The terminal sends a **GET PROCESSING OPTIONS** command with the data requested by the card in the PDOL (Tag '9F38') – if included in the Select response.

C Card Processing:

The ICC response may be formatted as 'Format 1' and just include the Application Interchange Profile and the AFL.

A second method of formatting the data ('Format 2') is to return a constructed data object. As a minimum, the card must return the Application Interchange Profile and the AFL; other data may be returned as well but the total length of the response message may not exceed 256 bytes.

T Terminal Processing:

The terminal must accept responses formatted as 'Format1' as well as responses formatted as 'Format2'.

In the response from the card, the AIP can be used to verify that the card is capable of continuing with the transaction; primarily that it supports a Cardholder Verification Method (CVM).

The Application File Locator (AFL) is required for the next EMV processing step.

The terminal must ignore and therefore need not check, the card's Card Authentication Method (CAM) capabilities.

Any further data items may be ignored by the terminal.

Read Application Data

The terminal reads the data indicated by the AFL.

Functional Requirements – Personal Card Reader
Application Commands and Processing

T Terminal Processing:

For each entry in the AFL, the terminal application issues one or more **READ RECORD** commands.

C Card Processing:

The ICC responds with the record data containing the data objects available for the given terminal type.

T Terminal Processing:

The terminal application parses the data read from the ICC and stores individual data objects in its internal database for use in the transaction process.

The terminal must keep only the data it needs for its application. Since the terminal will not perform 'Data Authentication', it does not need to retain whole records.

Offline Card Authentication

The PCR does not need to perform 'offline card authentication' as indicated in the settings of the Application Interchange Profile.

Process Restrictions

The PCR does not need to perform these tests because, irrespective of the outcome, the terminal will request an ARQC (but also accept an AAC if the ICC 'declined' the request) or an AAC.

Functional Requirements – Personal Card Reader
Application Commands and Processing

Cardholder Verification

The Chip Authentication Program requires the cardholder to present a valid PIN.

The only CVM implementation supported by the PCR is “Plaintext PIN verification performed by ICC” and must therefore be supported by the ICC.

If the CVM List read from the ICC contains one of the CVM codes ‘01’ or ‘41’, the transaction can proceed.

T Terminal Processing:

The Terminal first issues a **Get Data** command to obtain the current value of the Pin Try Counter (EMV Tag '9F17')

C Card Processing:

The ICC analyses the parameter received with the **Get Data** command.

It responds with a string that contains the current value of the Pin Try Counter ('9F17010x' where 'x' represents the value of the PTC).

T Terminal Processing:

If the value of the PTC = '0' or if the **Get Data** command fails, then the terminal must abort the transaction

If the value of the PTC > '0' the terminal proceeds with the transaction

Because the terminal must use ‘offline cleartext PIN validation’, the terminal must capture the PIN value via the PIN pad and construct a PIN Block according to the format rules specified in ISO 9564-1, Format 2 PIN Block.

The PCR sends this cleartext data structure to the ICC as an argument of the **VERIFY** command.

C Card Processing:

The ICC analyses the parameter received with the **VERIFY** command.

If the command carries a PIN Block in the clear, and the ICC supports this option, then the card retrieves the PIN value and validates the PIN.

T Terminal Processing:

No data is returned in response to the **VERIFY** command. The **sw1sw2** status word indicates the outcome:

- If offline PIN validation is successful (**sw1sw2** = 9000) the terminal will proceed with the transaction.

Functional Requirements – Personal Card Reader
Application Commands and Processing

- If offline PIN validation by the ICC failed and the ICC indicates a retry is permitted (**sw1sw2** returned by the ICC is in the range **63C1 - 63CF**) then the terminal must offer the cardholder another chance to re-enter their PIN.
- If all the offline PIN tries that are permitted by the ICC settings are consumed (**sw1sw2 = 63C0**) then the terminal must abort the transaction.

Terminal Risk Management

Since the issuer will process the transaction online anyway, there is no need to perform Terminal Risk Management.

Terminal Action Analysis

There is no need to implement a comparison of the TVR with the settings of the Terminal Action Codes as the result of the terminals actions will always go online to the card issuer.

First Action Analysis

An ICC may perform its own risk management to protect the issuer from fraud or excessive credit risk. Details of card risk management algorithms within the ICC are specific to the issuer and are outside the scope of EMV. However, because of the risk management process, an ICC may decide to:

- complete a transaction online or offline, or
- request a referral, or
- reject the transaction.

T Terminal Processing:

The terminal will ask the card to generate an ARQC Application Cryptogram.

The terminal must include the data identified by the ICC data element CDOL1 with the request. Different Card Specifications have different CDOL1 requirements - see the personalisation data for details.

The terminal builds the data string to be included with the **GENERATE AC** command. The tables given in Appendix A, "Data Structures", contain the recommended values for all static and transaction-dependent data.

C Card Processing:

The ICC performs its own Risk Management and generates an application cryptogram (AC).

T Terminal Processing:

Functional Requirements – Personal Card Reader
Application Commands and Processing

The response to the **GENERATE AC** command includes the AC and the other data held by the card that was included in the cryptogram generation:

- Cryptogram Information Data (CID)
- Application Transaction Counter (ATC)
- Optional Issuer Application Data (IAD).

The IOC may return other data elements; these may be ignored by the terminal application. The total length of the response message however must not exceed 256 bytes.

Both Format 1 (untagged) and Format 2 (tagged) GENERATE AC responses must be handled by the terminal.

**Functional Requirements – Personal Card Reader
Application Commands and Processing**

Terminal Online Processing

Online processing is normally performed to ensure that the issuer can review and authorize or reject transactions that are outside acceptable limits of risk defined by the issuer, the payment system, or the acquirer.

T Terminal Processing:

For PCR applications, the equivalent to the online processing stage prepares the SecureCode displayed to the cardholder, from the **GENERATE AC** response data. However, this does not occur until the transaction with the ICC has been completed, and hence is described below.

It can therefore be considered that the terminal will not perform any Online Processing.

Issuer to Card Script Processing

The PCR does not have the capability to provide command scripts and so the terminal does not perform this step.

Transaction Completion

The completion function closes processing of a transaction.

The terminal always performs this function – unless the transaction terminates prematurely due to errors.

T Terminal Processing:

If the ICC returned an AAC with the first **GENERATE AC**, then the transaction was 'declined offline' and no further processing is required.

If the ICC returned an ARQC with the first **GENERATE AC**, then the terminal should request the card to generate an AAC. The terminal must include the data identified by the ICC data element CDOL2 with the request. Different Card Specifications may have different CDOL2 requirements - see the personalisation data for details.

The terminal builds the data string to be included with the **GENERATE AC** command. The tables in Appendix A, "Data Structures", contains the recommended value for all static and transaction-dependent data.

C Card Processing:

The ICC will generate an application cryptogram (AC).

T Terminal Processing:

Functional Requirements – Personal Card Reader

Application Commands and Processing

The terminal has no use for the response and so it is ignored, as are any errors. However the transaction state within the ICC is now 'closed' and the card may now be powered off.

SecureCode Generation

When a successful transaction has been closed with the card, the terminal must generate the SecureCode to be presented to the cardholder. The token is generated from the response to the first, or only, **GENERATE AC** according to the IIPB value.

The PCR must generate the SecureCode, as detailed in Chapter 2, "Processing and Data Flows".

The SecureCode must only be displayed to the cardholder if the card is physically present in the terminal. This means that if ever the card is removed from the PCR while the SecureCode is being displayed, the terminal must clear its display and switch itself off.

Functional Requirements – Personal Card Reader
Application Commands and Processing

Exception Handling

Errors may be indicated in return codes from the ICC, be caused by cardholder action, or be detected by the PCR. In all cases, the PCR must stop processing the transaction and display an appropriate error message to the cardholder before turning itself off.

If errors are detected, the PCR must not generate, nor display, an SecureCode.

With the exception of the **VERIFY (PIN)** command, in the unlikely event that the PCR receives a status word response other than '0x9000' from a command sent to the ICC, it must indicate an error. The PCR must also indicate the error response code. Whilst of no use to the cardholder, the error response code may help to resolve an error condition on the card or PCR if that code can be communicated to the appropriate personnel.

The following error conditions also result in specific error messages.

- The application is blocked as a result of issuer action or by the internal processing of the card.
- The transaction is stopped because the cardholder pressed the **[Cancel]** key.
- The transaction is stopped because the cardholder removed the card from the PCR.
- The length of the IIPB does not match the length of the data returned by the ICC application.
- The IIPB defines too many bits to include in the SecureCode.
- The card failed to validate the PIN.

Functional Requirements – Personal Card Reader
Requirements and Recommendations

Requirements and Recommendations

Requirements

The following table summarizes the requirements that apply to the PCR:

Function	Requirements
Hardware Requirements	<p>Keypad</p> <p>The PCR has minimum requirements for a keypad, including</p> <ul style="list-style-type: none"> • numeric digits 0-9, • a [Proceed] (or 'OK' or 'Approval') key • a [Cancel] (or 'Abandon' or 'STOP') key. <p>If audible feedback for key presses it used, it must be monotonic (i.e. use a single tone).</p>
	<p>Display</p> <p>Depending on the size and nature of the display, prompts can be displayed:</p> <ul style="list-style-type: none"> • on a line above the data to be entered • to the left of the data to be entered • on the same line and replaced by the data being entered (or with a '*' for PIN entry). <p>The PCR must have at least a one-line display capable of displaying a minimum of 8 characters in a way that is clear to the cardholder.</p>
	<p>Character Set</p> <p>The PCR display must support the alphanumeric characters (A-Z, a-z, 0-9) and the following additional characters:</p> <p>* ? ! and , (comma) or . (full point)</p>
	<p>Card Reader</p> <p>The PCR must meet EMV Level 1 requirements for electro-mechanical ICC interfaces.</p>
	<p>EMV Commands</p> <p>The PCR must support the following limited subset of EMV commands required to implement the Chip Authentication Programme:</p> <ul style="list-style-type: none"> • SELECT • GET PROCESSING OPTIONS • Read Record • Get Data • VERIFY • GENERATE AC

Functional Requirements – Personal Card Reader
Requirements and Recommendations

Function	Requirements
	<p>PIN</p> <p>A PIN of between 4 and 12 digits is required, which must be entered/terminated by the use of a [Proceed] key.</p> <p>The value of the entered PIN must not be displayed in plain text, or be disclosed by visible or audible feedback dependent on the key pressed.</p> <p>The value of the entered PIN must never leave the handheld device, except for the purpose of being transferred to the IOC for off-line validation. This transfer must take place within the handheld device itself.</p> <p>The PCR must be constructed such that no information remaining in the PCR at the end of the transaction could, if ascertained, be used to determine any PIN which had been entered into the PCR, even given knowledge of all relevant data which has ever been available externally to the PCR.</p> <p>The PCR must be designed so that any component failure, or use of a component outside of its specification, shall not cause the disclosure of a PIN or PIN-related information.</p>
User Interface	<p>Cardholder Cancellation</p> <p>The cardholder must be able to cancel the transaction at any time, either by:</p> <ul style="list-style-type: none"> • removing the card • powering off the PCR, if applicable • pressing the [Cancel] key <p>Card Presence</p> <p>The PCR must not display any generated SecureCode if the associated card is not also physically present in the PCR. If the card is removed at any time, the PCR must terminate the transaction, restore all working variables to their initial default values and switch itself off.</p> <p>Challenge Length</p> <p>The PCR must accept a variable length Challenge of up to 8 digits.</p> <p>Completion of Data Entry</p> <p>The completion of any data entry – Challenge or PIN – must be indicated by the cardholder pressing the [Proceed] key.</p> <p>Correction of Data Entry</p> <p>All data entry – Challenge, PIN – must be correctable prior to the cardholder pressing the [Cancel] key.</p> <p>Token Display</p> <p>The SecureCode must be displayed as a numeric value of up to 8 digits. The use of formatting separators for readability is optional.</p>

Functional Requirements – Personal Card Reader
Requirements and Recommendations

Function	Requirements
	Minimum Token Display Time The SecureCode must be displayed for a minimum of 30 seconds.
PIN Entry	Cardholder Feedback The PCR must use the '*' for visual feedback of PIN digits entered. The PCR must not provide any audible feedback that could disclose the value of the digits entered. Invalid PINs The PCR must indicate any invalid PIN entry to the cardholder, together with the number of PIN attempts remaining. The PCR must allow a maximum of no more than three PIN retries, even if there are more attempts remaining on the card. The PCR must terminate the transaction if PIN entry fails and there are no PIN tries remaining.
Transaction Processing	IIPB Length The length of the IIPB must match the length of the data fields (without Tag and Length) returned by the ICC Application. IIPB Effective Length When an unconnected PCR obtains the IIPB from the card it must ensure that its effective length – the number of bits set to 1, indicating data to be transferred – does not exceed 26. (The maximum number of bits that can be represented by a maximum 8-digit SecureCode). EMV Flow The PCR must conduct an EMV transaction dialogue with the card as defined in this specification, without interruptions that might adversely affect the card's expectation of the transaction flow. Shortcuts allowed from the EMV specification are indicated in the text of this specification.

Recommendations

The following table summarizes the recommendations that apply to the PCR:

Function	Recommendations
PIN Entry	Blocked PIN Check The PCR is recommended to determine if the card's PIN is blocked prior to accepting any cardholder input.

60475639 . 060403

**SecureCode(Authentication Application
Requirements and Recommendations**

4

SecureCode™ Authentication Application

This chapter gives an overview of the authentication application and describes the personalization issues.

60475639 . 060403

SecureCode(Authentication Application)

Introduction.....	1
Authentication of card and cardholder.....	1
Card Issuance	2
PIN Management	2
Keys	3
Script Processing.....	3
Summary of Authentication Application Personalization	3
Recommended Personalization settings.....	3

Introduction

The card must contain the M/Chip payment application as the primary application associated with the card. The M/Chip authentication application is secondary to this application and may share some of the application data defined for the payment application. The issuer may use the same offline PIN for both applications to provide the cardholder with a "seamless" experience while keeping the two applications separate. The authentication application is used for the authentication of remote transactions.

The applications are personalized to perform in the appropriate environment. For face-to-face transactions, the payment application must confirm the card is being used in a valid terminal device and perform card risk management functions. The authentication application eliminates these features so that the card can be used in remote online transactions with no fear that the application can be used fraudulently in a face-to-face environment. It is the elimination of these features that provides the ability to create unique, authenticable tokens or SecureCodes that are only 8 digits in length.

The authentication application takes advantage of EMV principles and capabilities since EMV already solves the problem of remote authentication between the cardholder and the issuing bank. Consequently, the authentication application uses this technology to pave the way for wide acceptance of smart card-based authentication and to protect issuer investments in the infrastructure for EMV. Many of the issuer facilities implemented for EMV payment transactions are re-used with the authentication transactions, but the two types of transactions, payment and authentication should be kept clearly separate and distinct from each other.

Authentication of card and cardholder

An authentication transaction is a special form of an EMV transaction. It uses the same sequence of execution, principles of data abstraction and smart card commands. However, it leaves out most of the offline functions in EMV, namely offline data authentication, processing restrictions, terminal risk management, terminal action analysis, card action analysis, and issuer script processing. Offline PIN verification is performed for the purpose of verifying the correct entry of the PIN. The transaction is forced online for validation of the card actions. The process of authenticating the card and cardholder at a remote device is as follows:

1. The client device prompts the cardholder for the PIN.
2. The cardholder submits the PIN to the card application along with certain transaction-specific parameters (challenge or unpredictable number) that are unique to the transaction. The transaction data elements are indicated in the data object list read from the card. If data elements used by the card are not available, zero or default values are substituted.
3. The client device verifies that the PIN was entered correctly.

SecureCode(Authentication Application

- If not, the client requests the cardholder to reenter their PIN and notifies the cardholder of the number of PIN tries remaining.
 - If the number of PIN tries has been exhausted, the client device does not create a SecureCode. Note: if this occurs, the application is locked and can no longer be used for authentication.
4. The card application uses the requested data elements and generates a cryptogram as the message authentication code (MAC) across these data elements and other internal data, using a secret session key generated internally in the smart card.
 5. The Authentication Cryptogram (AC) is returned to the client device and the client device formats the SecureCode.
 6. Finally the device displays the SecureCode™, or if the device is connected to the personal computing device, it returns the SecureCode™ in the APDU response.

Card Issuance

The issuer must configure the two M/Chip applications on the card, payment and authentication. The payment application is personalized according to the processing methods and modes desired by the issuer. The authentication application must be personalized as defined in this section and in the Appendices. The applications will be loaded during the same initialization process, although the card issuer could handle this in separate steps.

PIN Management

The issuer may choose to use a separate PIN for complete separation, but there is a risk since the PIN on the authentication application cannot be changed. If a separate PIN is used, the PIN will be generated (or applied) during the personalization process and mailed to the cardholder, preferably with the payment PIN to avoid confusion. The choice of a separate or common PIN is an issuer decision.

When using separate PINs, issuers must decide whether the cardholder will be able to change the PIN and implement appropriate mechanisms to allow that. Issuers must also be aware of the possibility of locking the authentication application in the event of too many failed PIN attempts and again implement appropriate mechanisms if they wish to enable the unblocking of such applications.



Blocked authentication applications have their PIN reset by processing a script. Not only must issuers implement the mechanism, typically special in-branch terminals, to deliver this script, they must also ensure that script counters are maintained for particular cards at the Authentication Request Server.

SecureCode(Authentication Application
Summary of Authentication Application Personalization

Keys

One major issue is the choice of issuer master keys for each application - MasterCard policy⁷ is that separate issuer master keys are required for security. The Security Module accessed by the Authorisation Request Server will have to store and maintain the authentication key.

Script Processing

Although the authentication application may support script processing, it is not possible to use script processing when conducting an authorisation transaction. Issuers that employ a specific terminal, e.g. in a bank branch, to update a card with scripts, will need to ensure that script counters are updated appropriately in the Authentication Request Server's card database.

Summary of Authentication Application Personalization

The authentication application does not contain functions for Dynamic Data Authentication (DDA) or Static Data Authentication (SDA) because the transaction will be conducted as an online transaction.

Recommended Personalization settings

Appendices B and C document the personalization settings to be used by the issuer for M/Chip 2.1 and M/Chip 4.0, respectively. For M/Chip Select, MasterCard International specifies the data elements used in cryptogram generation. The data elements used in cryptogram generation are set by the CDOL_AC_Truncation_lengths parameters defined in the Personalization Data Map for M/Chip.

Due to the special nature of the authentication environment, the following EMV defined functions are not used during an authentication transaction:

- Offline Data Authentication
- Processing Restrictions
- Terminal Risk Management
- Capture Request and Response
- Issuer Script Processing & Completion

⁷ See M/Chip 4 Security & Key Management, Vsn 1.0 Oct 2002

CONFIDENTIAL DRAFT – NEW PRODUCT ENGINEERING

3-D SECURE™ CHIP AUTHENTICATION PROGRAM

PREFACE

5

SecureCode™ Chip Authentication for 3-D Secure™

This chapter provides a description of the MasterCard 3-D Secure chip authentication application (CAA) as used for MasterCard SecureCode™. It identifies the role of this option in the overall MasterCard SecureCode program and describes the implementation of the CAA with the MasterCard 3-D Secure environment.

Introduction.....	1
MasterCard SecureCode Program.....	1
Download implementation.....	1
MasterCard implementation of 3-D Secure™	1
Reference documents	1
MasterCard SecureCode documents	1
MasterCard 3-D Secure documents.....	2
MasterCard Chip Authentication Program for 3-D Secure™	3
General Description.....	3
SecureCode™ Chip Authentication.....	3
Benefits.....	4
Merchant Benefits.....	4
Acquirer Benefits	5
Issuer Benefits	5
Cardholder Benefits	5
3D Secure Operating Principles.....	6
3-D Secure Authenticated Transaction Flow.....	9
Cardholder Authentication (Step 8)	11
3-D Secure Entities.....	12
Cardholder	13
Cardholder Authentication Page of the ACS	13
Personal Card Reader	14
ICC	14
Acquirer.....	14
Issuer	14

60475639 : 060403

SecureCode(Chip Authentication for 3-D Secure™
Introduction

Introduction

MasterCard SecureCode Program

Each of the cardholder authentication solutions offered under the SecureCode program differ slightly in technology, however, converge around the use of Universal Cardholder Authentication Field (UCAF) for data transport. The UCAF is used in two basic infrastructures:

- the download implementation, and
- the MasterCard implementation of 3-D Secure™.

Download implementation

Both the PC Authentication Program and current Chip Authentication Program (CAP) solutions rely upon UCAF hidden fields embedded on the merchant's order confirmation page to trigger pop windows for cardholder authentication and to exchange cardholder authentication data once the cardholder has been authenticated. Each of these solutions are applet-based but differ in terms of the authentication approach utilized to confirm the identity of cardholder. The PC Authentication Program is primarily a password-based platform whereas the CAP solution utilized an EMV smart card with PIN to create a cryptogram that is then used to verify the cardholder. Both options require the use of download software present on the cardholder's device.

MasterCard implementation of 3-D Secure™

The 3-D Secure™ option uses a pop-up box for the entry of the cardholder SecureCode within the operational techniques defined for 3-D Secure™. The SecureCode may be either a static passcode or may be a one-time dynamic value created by the Chip Authentication Application. The SecureCode is verified by an Access Control Server. In either mode, the Access Control Server controls the format and presentation of the pop-up window so that cardholders do not have to download and install software on their device.

Reference documents

The documents that define the MasterCard SecureCode program and the MasterCard Implementation of 3-D Secure are listed below. This document assumes that the reader has access to and knowledge of the contents of these documents. This document only identifies differences from the definitions provided in the reference documents.

MasterCard SecureCode documents



60475639 • 060403

SecureCode(Chip Authentication for 3-D Secure™

MasterCard 3-D Secure documents

60475639 4060403

SecureCodeTM Chip Authentication for 3-D SecureTM
MasterCard Chip Authentication Program for 3-D SecureTM

MasterCard Chip Authentication Program for 3-D SecureTM

General Description

CAP for 3-D SecureTM (CAP-3DS) is one of several possible secure authentication methods that take advantage of MasterCard's SecureCode infrastructure. It consists of the following elements:

- Issuer-provided cardholder interfaces that access the authentication application.
- Generation of specific CAP data that is used in lieu of a 3-D SecureTM static passcode to verify the authenticity of the card and cardholder.
- Cardholder verification and card authentication procedures based on the cardholder providing their PIN that the card must verify.

This solution is intended to be layered on top of the existing 3-D SecureTM version 1.0.2 compliant issuer ACS platform with no changes at all to the core protocol or messages. The changes to the ACS will be in the use of an Authentication Request Service by the ACS to request and validate a SecureCodeTM from the PCR.

The issuer will have to arrange to supply the cards and the PCRs to their cardholders together with instructions on their use in the 3-D Secure environment.

The following elements of transaction processing are all based on the MasterCard SecureCodeTM infrastructure:

- Merchant request for and collection and processing of AAV.
- Acquirer acceptance and processing of the AAV data.
- Network development to enable the payment system to include support for carrying AAV data within the transaction message.

Authorization of e-commerce transactions based on issuer validation of the AAV data.

SecureCodeTM Chip Authentication

CAP meets the goals of cardholder authentication in those transaction environments that traditionally suffer from high levels of disputed transactions. Chargebacks can arise when the cardholder disputes the transaction and no strong evidence can be provided by the acquirer or issuer that the genuine cardholder actually engaged in the transaction. CAP offers a mechanism for securing electronic commerce and specifically the Internet channel by:

- strongly authenticating the cardholder at the point-of-interaction (POI), and
- providing explicit evidence of the presence of both the card and the cardholder, and
- optionally, providing proof the acceptance of a transaction by the cardholder.

**SecureCode(Chip Authentication for 3-D Secure™
MasterCard Chip Authentication Program for 3-D Secure™**

Within this environment, MasterCard has a number of goals:

- to reduce chargebacks for Reason Code 37 – No Cardholder Authorization
- to support both credit and debit transactions
- to leverage existing issuer security scheme investments
- to minimize the impact on acquirer systems
- to ensure rapid adoption by merchants, and
- to instill confidence in cardholders in the security and privacy of electronic commerce.

Benefits

The implementation of MasterCard CAP for 3-D Secure benefits all parties in the transaction chain, including the merchant, the acquirer, the issuer and the cardholder.

CAP standardizes the use of issuer-defined chip authentication data within the infrastructure specified by the MasterCard SecureCode program. This provides a security mechanism to issuers and cardholders that is independent of the merchant and acquirer, but is the basis to guarantee their financial risk.

Merchant Benefits

The merchant is the principal beneficiary of the MasterCard SecureCode Program. The main driver for the program is the liability shift for 'cardholder not authorized' chargebacks – introduced by MasterCard for all merchants whose systems (and related acquirer systems) support the SecureCode Program. To the merchant, the main benefits of using the SecureCode Program are:

- potential access to an enhanced payment guarantee for online transactions (proving certain conditions are met, and the issuer approves the transaction)
- support for MasterCard credit and debit cards including Maestro, thus opening up many new international transaction opportunities
- ease of implementation and minimal cost impact on merchant systems
- use of the standard message infrastructure for both new and existing platforms, supporting a range of cardholder authentication schemes and transaction channels.

CAP offers the additional benefit of providing the merchant with evidence of both card and cardholder authentication, thus preventing cardholders from:

- denying that their card was used, and
- denying that they explicitly authorized the transaction.

60475629 • 060403

**SecureCode(Chip Authentication for 3-D Secure™
MasterCard Chip Authentication Program for 3-D Secure™**

Acquirer Benefits

Acquirers benefit indirectly from MasterCard SecureCode in that there will be fewer Internet-related chargebacks to process. With potentially higher transaction volumes over the Internet, it is expected that acquirers will also benefit from increased fee revenues.

Issuer Benefits

Despite the shift in liability and the need to cover the costs of providing cardholders with a Personal Card Reader, issuers will benefit from:

- higher volumes, as Internet activity increases
- lower chargeback processing costs, and
- the possibility of using the same means of secure authentication for other products and remote services.

Issuers will benefit from a significant reduction in operating costs relating to dispute management and chargeback processing. The card and cardholder authentication performed when the transaction occurs using CAP greatly reduces the cardholder's ability to repudiate a transaction (resulting in a chargeback for Reason Code 37, No Cardholder Authorization).

Given that the chip-based functions described in this document essentially provide a means of verifying the cardholder presence to the issuer, the same service can also be leveraged in remote banking environments ('e-banking' and 'm-banking'). This can provide issuers with a consistent and secure consumer authentication method across a variety of products, services and environments.

Cardholder Benefits

Cardholder benefits are less obvious to quantify, as the incentive for this scheme is to reduce merchant losses due to cardholder chargebacks. However, there are indirect cardholder benefits that can be identified and these should be emphasized by issuers:

- There can be a reduction in the risks perceived by the cardholder in using their credit/debit card as a means of payment over the Internet. The use of a SecureCode created under the cardholder's control provides a secure and private mode of operation.
- More merchants will be prepared to do business over the Internet, leading to a further uptake of e-commerce facilities, resulting in increasing choice for consumers and stimulated competition for business.
- There will be a significant reduction in genuine 'not me' transactions, reducing the need for cardholders to have to engage in such disputes.

3D Secure Operating Principles

The following figure illustrates the 3-D Secure™ architecture and the message flows involved in a chip-authenticated transaction. The dark bar indicates the areas that are in the scope of this document, namely the authentication mechanism between Card/Cardholder and the Issuer's Access Control Server.

This flow assumes that:

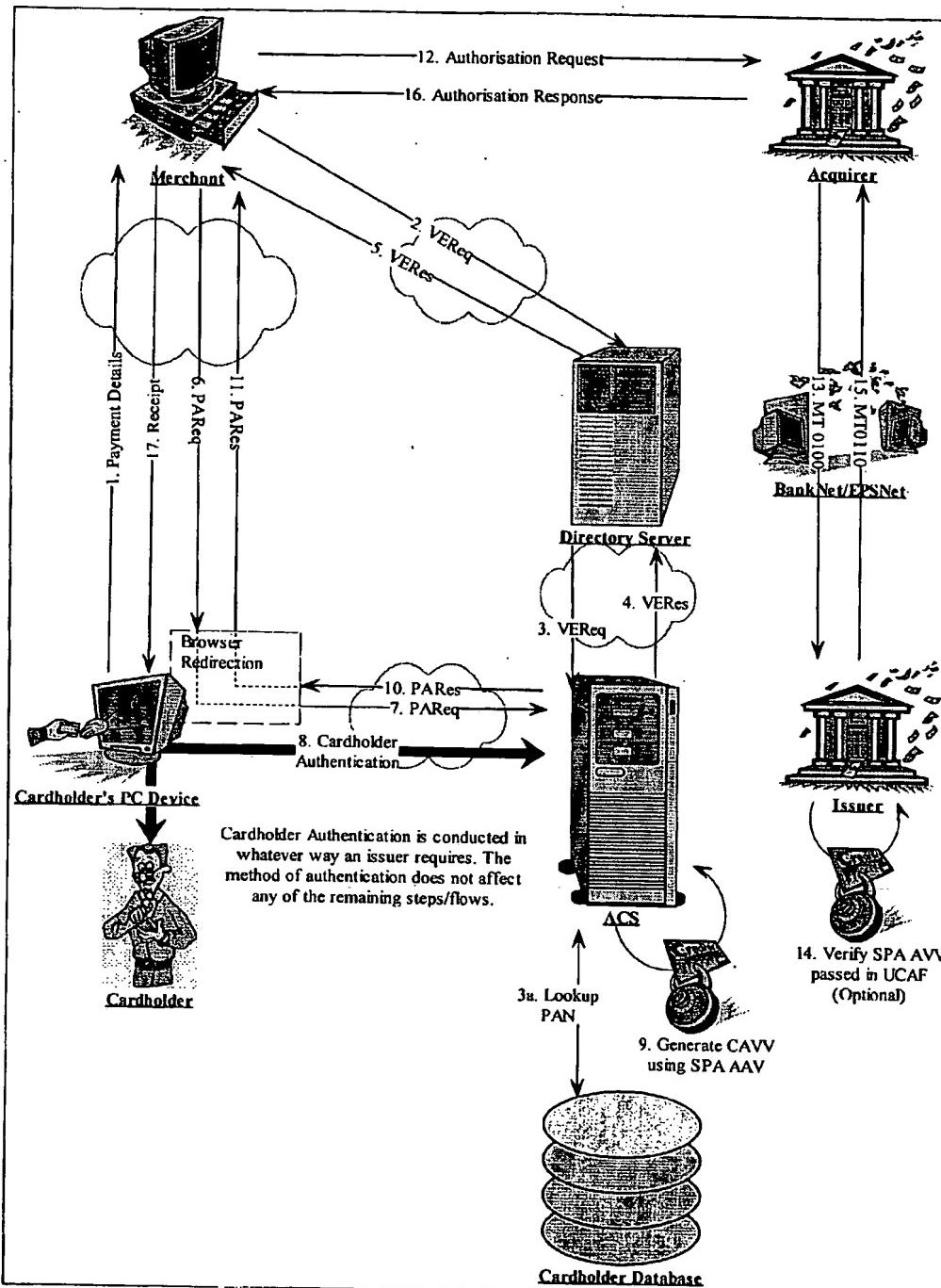
- prior to conducting a transaction, the cardholder has registered with their issuer for the service, and has a chip card and a compatible Personal Card Reader
- the cardholder wishes to make a purchase, has selected the required goods or services and has initiated the 'checkout' process on the merchant's Web site
- the merchant has already requested the cardholder to provide details of their payment card, which have been entered onto the merchant's Web site in a protected manner.

The detailed description of the transaction flow is given in the MasterCard SecureCode and the 3-D Secure documents. Those documents specify the security considerations of the operational process.

60475639 . 060403

SecureCode(Chip Authentication for 3-D Secure™
3D Secure Operating Principles

SecureCode(Chip Authentication for 3-D Secure™
3D Secure Operating Principles



3-D Secure Authenticated Transaction Flow

Each of the steps of the transaction flow in Figure 1.1 is described below. The chip authentication process affects only step 8, the creation and entry of the SecureCode. The standard 3-D Secure version 1.0.2 message formats and data formats are used as described in the MasterCard 3-D Secure Implementation Guide document. Specifically, the CAVV carried is 28 characters long and contains the 20 byte field defined for 3-D Secure in base64 encoding. The use of the chip application for authentication is indicated in the "Authentication Mode" field (value '2').



Note The format of the AAV is the same for all 3-D Secure modes of operation, static passcode or CAP-3DS.

1. Payment Details: Cardholder to Merchant (HTTPS/POSTed Form)
 The cardholder having browsed and selected items, 'checks out' supplying personal details, including – of particular interest in this scope – payment card details to the merchant, i.e., the embossed card number (PAN).

2. VEReq (Verify Enrollment Request): Merchant to Directory Server (DS) (HTTPS/POST)

The merchant's 3-D Secure processing software sends a VEReq to the appropriate brand directory server to determine if the PAN is enrolled in the issuer's 3-D Secure program.



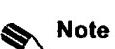
Note Merchants are encouraged to maintain, on a daily basis, a local cache of the directory server in order to avoid consulting the directory server for every payment. The cache will contain all eligible brand card ranges participating in the program. Use of the cache option will prevent calls to the directory for those instances when the cardholder PAN is not eligible to participate in the program.

3. VEReq: Directory Server to Access Control Server (ACS) (HTTP/POST)

Based on card ranges, the directory server passes the VEReq onto the appropriate ACS. The ACS determines whether or not the card (Cardholder PAN) is enrolled in 3-D Secure.

4. VERes (Verify Enrollment Response): ACS to DS (Response to HTTPS/POST)

The ACS returns an indication of whether the specific PAN is enrolled in the system, and, if so, the URL that will be used to redirect the cardholder's browser in order to perform authentication towards the ACS.



Note The ACS returns a unique Account Identifier, which may not be the PAN, that is used by the ACS when contacted by the Cardholder with a PReq to identify the payment card in question. This Account Identifier must match the PAN of the actual card used on a 1 to 1 basis in order that the key may be correctly generated so that the SecureCode™ can be verified.

5. VERes: DS to Merchant (Response to HTTPS/POST)

The DS returns that response to the merchant.

**SecureCode(Chip Authentication for 3-D Secure™
3D Secure Operating Principles**

6. **PReq (Payer Authentication Request): Merchant to Cardholder (HTML Page)**
The merchant's 3-D secure processing software constructs a PReq and Base64 encodes it and places it into a HTML form field (PaReq). The merchant URL to which the cardholder's browser must be redirected after authentication is placed into a HTML form field (TermUrl) and any merchant state data that they might require when contacted via TermUrl is also placed into a HTML form field (MD). A HTML page is then returned to the cardholder as the response to the posting of their payment details. The POST address for this form is the URL of the ACS, as per the VERcs.
7. **PReq: Cardholder to ACS (HTT/POST)**
The page returned by the merchant typically opens up an additional small 'pop-up' window, which then POSTs the form data filled in by the merchant to the ACS.
The ACS looks up the cardholder details and determines the authentication mechanism to use for this particular payment card and in the case of Chip Authentication the type of challenge required for the authentication.
8. **Cardholder Authentication: ACS to Cardholder to ACS (HTML Page followed by HTTPS/POST)**
Cardholder authentication is conducted in a manner appropriate to the particular issuer and/or cardholder.



In the case of chip authentication, the authentication process is carried out as described in the Authentication Request Server chapter.

Access Control Servers may support more than one type of cardholder authentication, but only one method per card is allowed. The ACS has to determine the method to use from the information stored for the card/cardholder.

The process for authentication by use of the chip card and the Personal Card Reader is the subject of this specification.

9. **Generate CAVV: ACS**
On successful validation via the employed authentication mechanism, the ACS constructs a SPA AAV as outlined in the SPA Algorithm for MasterCard's Implementation of 3D Secure specification. This value will be placed in the CAVV subfield of the PARes for return to the merchant.
10. **PARes (Payer Authentication Response): ACS to Cardholder (HTML Page)**
The ACS constructs a PARes, including the AAV and a message signature, and Base64 encodes it and places it into a HTML form field (PaRes). The merchant data received in the PReq is also returned to the merchant in a HTML form field (MD). The POST address for the form in this page is the URL of the merchant, as per the PReq's TermUH field.
11. **PARes : Cardholder to Merchant (HTTIPS/POST)**
The page returned by the ACS then POSTs the form data filled in by the ACS to the

**SecureCode(Chip Authentication for 3-D Secure™
3D Secure Operating Principles**

merchant, where the merchant's 3-D secure processing software may verify the message signature generated by the ACS.

12. Authorisation Request: Merchant to Acquirer (Proprietary Communication)
The Merchant includes the AAV received in the PAREs in the authorisation request sent to their Acquirer, along with the standard authorisation request data.
13. MT0100/0200: Acquirer to Issuer (BankNet)
The acquirer extracts the authentication data and inserts it into the UCAF field within authorization message and sends to the appropriate MasterCard authorization network.
14. Verify SPA AAV: Issuer
The issuer may verify the AAV value contained in the UCAF field of the authorization message to ensure that cardholder authentication took place with the given card.
15. MT0110/0210: Issuer to Acquirer (BankNet)
The standard authorisation processing is performed and the response returned to the Acquirer.
16. Authorisation Response: Acquirer to Merchant (Proprietary)
The merchant receives the authorisation response from their acquirer.
17. Response/Receipt: Merchant to Cardholder (HTML)
The merchant returns an indication to the cardholder as to whether their payment has been accepted.

Cardholder Authentication (Step 8)

The ACS controls the interface with the cardholder and directs the cardholder's use of the PCR. Based on the configuration parameters within the ACS, the issuer may implement a "one-time passcode" SecureCode or may implement a "transaction acceptance" SecureCode. The difference is that the cardholder must enter a challenge on an unconnected PCR before entering their PIN in order to accept a specific transaction. This step is not required with the one-time passcode. (Note: There is no difference to the cardholder when a connected reader is used.)

SecureCode(Chip Authentication for 3-D Secure™
3D Secure Operating Principles

3-D Secure Entities

The following entities are involved in the lifetime of a chip authenticated transaction:

- **Cardholder** – The cardholder initiates the transaction and is responsible for entering data into the merchant's payment Web pages, the Personal Card Reader, and the Cardholder Authentication Page. The cardholder must enter their PIN in the PCR in order for the PCR to create a SecureCode using data from the chip authentication application.
- **Merchant** – The merchant supplies the necessary data to start the authentication transaction, and receives the resultant authentication data to forward, via their acquirer, to the issuer for verification. The merchant operates the normal 3-D Secure process.
- **Cardholder Authentication Page** – The Cardholder Authentication Page is the web page presence of the ACS. It displays the relevant data and instructions supplied by the ACS and interacts with the cardholder. The Cardholder Authentication Page is returned by the ACS and runs as part of the Internet browser (i.e., a 'pop-up' window). This page, in addition to the standard display information for MasterCard's implementation of 3-D Secure, may also include a challenge if required by the issuer.
- **Personal Card Reader** – The Personal Card Reader interacts with the cardholder and the ICC to produce a SecureCode that is passed, indirectly, to the issuer through the ACS. Depending on the type of reader and type of transaction, the cardholder may need to enter a challenge displayed on the issuer generated authentication pop-up window before entering the required PIN. The cardholder must enter the displayed value on the Cardholder Authentication Page web page as the SecureCode™. (Note: data entry, other than PIN entry, is not necessary with connected readers.)
- **ICC** – The EMV-compliant chip card authenticates the cardholder by means of PIN verification, and generates a suitable cryptogram based on data supplied by the Personal Card Reader.
- **Acquirer** – The acquirer accepts the transaction data from a merchant and forwards it to the issuer via the appropriate network. The acquirer follows the normal 3-D Secure process.
- **Issuer** – The issuer distributes Personal Card Readers to those cardholders that are signed up for the 3-D Secure chip authentication program. Importantly, the issuer may optionally validate the authentication data (AAV) transmitted in the UCAF field within the authorization request from the acquirer – according to the rules of that issuer.
- **Access Control Server** - The issuer operates the Access Control Server as specified for 3-D Secure with additional ability to present the Cardholder Authentication Page and receive the SecureCode from the PCR either directly or indirectly from the cardholder. The ACS verifies the validity of the SecureCode by using an Authentication Request Service which:

**SecureCode(Chip Authentication for 3-D Secure™
3D Secure Operating Principles**

- a. extracts the data known only to the chip (ATC and indicator for the type of cryptogram) from the SecureCode
- b. regenerates the cryptogram and
- c. compares the result with the partial cryptogram in the SecureCode.
- **Enrollment Server** - The enrollment server and enrollment process are the same as the normal 3-D Secure process. There may be a requirement for the cardholder to indicate that the PAN is a chip card and that the chip will be used in place of static password. This could be a cardholder decision or an issuer decision or perhaps a configuration option. The issuer will have to indicate the format of the SecureCode and whether or not a challenge is displayed for cardholder entry in the PCR. Ideally, the majority of these decisions will be configurations options from which the issuer can choose.
- **Directory Server** - The Directory Server operates in the normal 3-D Secure mode.

Cardholder

In order to use the chip authentication scheme, the cardholder must be in possession of an EMV-compliant chip-based payment card with the Authentication Application and a Personal Card Reader. The issuer supplies the PCR to the cardholder, and must assure that the cardholder enrolls in the 3-D Secure chip authentication scheme.

How a cardholder is enrolled in the program must be determined by the issuer. Similarly, issuers must decide how the solution will be 'sold' to their cardholders. It is the responsibility of the issuer to educate the cardholder in a) how the process works (PIN entry) and b) to be careful to only enter their PIN when an appropriate request is displayed and they are expecting to perform a transaction.

Cardholder Authentication Page of the ACS

The Cardholder Authentication Page presents the secure face of the MasterCard Chip authentication scheme to the cardholder and is responsible for:

- requesting the cardholder to use the chip card in the PCR to create a SecureCode
- if required, requesting the cardholder to enter the displayed challenge in the unconnected reader
- if required, including the embedded software component (e.g., an ActiveX Control) in the web page to interact with a connected PCR
- receiving the SecureCode in response
- populating the return data.

SecureCode(Chip Authentication for 3-D Secure™ 3D Secure Operating Principles

Personal Card Reader

The Personal Card Reader (PCR) is a device used to interact with the cardholder's chip-based payment card. It enables:

- offline PIN entry and PIN verification
- creation of a SecureCode for the authentication of data cardholder's acceptance of an e-commerce transaction.

There are two types of card reader:

- **Unconnected Card Reader** – The cardholder is required to manually transfer data to and from this type of reader. The cardholder enters the PIN on the PCR and then copies the SecureCode into the Cardholder Authentication Page. If a transaction is to be approved, the cardholder is prompted to enter a challenge before entering their PIN. An issuer may implement a cardholder authentication page that does not use a challenge, but they must understand the associated risk of possible disputes.
- **Connected Card Reader** – Data is sent to and retrieved from this type of reader automatically by an embedded software component downloaded with the Cardholder Authentication Page. The cardholder simply visually verifies the authentication transaction information on the HTML page, enters the PIN on the EMV-L2 compliant PCR and waits for a response from the ACS.

ICC

The ICC must be an EMV-compliant chip card. Issuers may implement whatever version of MasterCard payment application technology they choose on the ICC. The chip authentication application will share the use of this technology to provide a second application for remote authentication.

Acquirer

In the context of SecureCode and 3-D Secure, acquirers maintain relationships with their 3-D Secure-enabled merchants. This means that acquirers have educated their merchants in the advantages of the liability shift brought about by SecureCode and the necessary (though minor) changes required to their existing e-commerce systems to support cardholders. Additionally, acquirers must adhere to the guidelines and requirements outlined in the MasterCard SecureCode Enrollment and Implementation Guide.

Issuer

The issuer is responsible for educating their cardholders in the proper use of the card and the PCR, especially when to enter the (optional) challenge and their PIN. Additionally, issuers must adhere to the guidelines and requirements outlined in the MasterCard SecureCode Enrollment and Implementation Guide.

60475629 . 060403

Terminal and Transaction Related Data
3D Secure Operating Principles

A

Terminal and Transaction Related Data

This appendix provides a formal definition of all data structures personalized at the Terminal or created at the Terminal when processing a Chip Authentication transaction.

Terminal and Transaction Related Data

Introduction	1
Static Terminal Data	1
Acquirer Identifier (9F01)	1
Additional Terminal Capabilities (9F40)	1
Application Identifier (AID) (9F06)	1
Application Version Number (9F09)	1
Interface Device (IFD) Serial Number (9F1E)	1
Merchant Category Code (9F15)	2
Merchant Identifier (9F16)	2
Terminal Action Code - Decline	2
Terminal Action Code - Default	2
Terminal Action Code - Online	2
Terminal Capabilities (9F33)	2
Terminal Country Code (9F1A)	2
Terminal Floor Limit (9F1B)	2
Terminal Identification (9F1C)	2
Terminal Type (9F35)	3
Transaction Related Terminal Data	4
Amount, Authorised (Binary) (81)	4
Amount, Authorised (Numeric) (9F02)	4
Amount, Other (Binary) (9F04)	4
Amount, Other (Numeric) (9F03)	4
Amount, Reference Currency (Binary) (9F3A)	4
Authorisation Response Code (8A)	4
Cardholder Verification Method (CVM) Results (9F34)	4
Terminal Verification Results (95)	4
Transaction Currency Code (5F2A)	5
Transaction Currency Exponent (5F36)	5
Transaction Date (9A)	5
Transaction Reference Currency Code (9F3C)	5
Transaction Reference Currency Exponent (9F3D)	5
Transaction Sequence Counter (9F41)	5
Transaction Status Information (9B)	5
Transaction Time (9F21)	5
Transaction Type (9C)	5
Unpredictable Number (9F37)	6

60475639 • 060403

Terminal and Transaction Related Data

Introduction

The tables in this appendix provide formal definitions for all data object that need be personalized at a terminal used for the Chip Authentication service.

For details on the meaning and encoding specifications of the data elements, the reader is referred to the related EMV specification documents:

EMV2000 Integrated Circuit Card Specifications for Payment Systems - Book 3,
Application Specification; Version 4.0 - December, 2000.

EMV2000 Integrated Circuit Card Specifications for Payment Systems - Book 4,
Cardholder, Attendant, and Acquirer Interface Requirements; Version 4.0 - December,
2000.

Static Terminal Data

Acquirer Identifier (9F01)

Must be set to '000000000000'

Additional Terminal Capabilities (9F40)

The Additional Terminal Capabilities are not interpreted by the M/Chip applications; must be set to '0000000000'.

Application Identifier (AID) (9F06)

The Application Identifier the terminal application must use to select the Card Application providing the Chip Authentication service. It is set to the following value:

0xA000000048002

Application Version Number (9F09)

Must be set to '02'

Interface Device (IFD) Serial Number (9F1E)

Must be set to "00000000"

60475639 .060403

Terminal and Transaction Related Data
Static Terminal Data

Merchant Category Code (9F15)

Must be set to '0000'

Merchant Identifier (9F16)

Must be set to "0000000000000000"

Terminal Action Code - Decline

The Terminal Action Code - Decline is not to be used for the Chip Authentication; may be set to '0000F80000'

Terminal Action Code - Default

The Terminal Action Code - Default is not to be used for the Chip Authentication; may be set to '0000000000'

Terminal Action Code - Online

The Terminal Action Code - Online is not to be used for the Chip Authentication; may be set to 'F8F804F8F0'

Terminal Capabilities (9F33)

Must be set to '208000'

Terminal Country Code (9F1A)

Must be set to '0000'

Terminal Floor Limit (9F1B)

Must be set to '00000000'

Terminal Identification (9F1C)

Must be set to "00000000"

60475639 . 060403

Terminal and Transaction Related Data

Static Terminal Data

Terminal Type (9F35)

Must be set to '34'

Terminal and Transaction Related Data
Transaction Related Terminal Data

Transaction Related Terminal Data

Amount, Authorised (Binary) (81)

The default value must be set to '00000000'.

Amount, Authorised (Numeric) (9F02)

The default value must be set to '000000000000'.

Amount, Other (Binary) (9F04)

The Amount, other is not used for the Chip Authentication service but is requested by the Card Application; must be set to '00000000'

Amount, Other (Numeric) (9F03)

The Amount, other is not used for the Chip Authentication service but is requested by the Card Application; must be set to '000000000000'

Amount, Reference Currency (Binary) (9F3A)

The Amount, Reference Currency is not used for the Chip Authentication service; must be set to '00000000'

Authorisation Response Code (8A)

When requested by the Card Application in the CDOL1, the terminal returns a value set to '0000'; when requested in the CDOL2, the terminal returns "Z3" (Unable to go online - Offline Declined).

Cardholder Verification Method (CVM) Results (9F34)

The outcome of the Offline PIN validation; should be set to 'nnnn01' (PIN Validation OK) or 'nnnn02' (PIN Validation failed) where 'nnnn' is set to the CVR obtained from the CVM list encoded in the Card Application.

Terminal Verification Results (95)

Must be set to '8000000000'

60475639 1060403

Terminal and Transaction Related Data

Transaction Related Terminal Data

Transaction Currency Code (5F2A)

The default value must be set to '0000'.

Transaction Currency Exponent (5F36)

The default value must be set to '00'.

Transaction Date (9A)

The default value must be set to '000000'.

Transaction Reference Currency Code (9F3C)

The default value must be set to '0000'.

Transaction Reference Currency Exponent (9F3D)

The default value must be set to '00'.

Transaction Sequence Counter (9F41)

The default value must be set to '0000'.

Transaction Status Information (9B)

The value of the TSI for the terminal involved with the Chip Authentication Service must be set to '0000'.

Transaction Time (9F21)

The value of the Transaction Time for the terminal involved with the Chip Authentication Service must be set to '000000'.

Transaction Type (9C)

The value of the Transaction Type for the terminal involved with the Chip Authentication Service must be set to '00'.

60475639 • 060403

Terminal and Transaction Related Data
Transaction Related Terminal Data

Unpredictable Number (9F37)

The default value of the Unpredictable Number is set to '00000000'; note that the value of the UN must be overwritten with the binary value of the Challenge, if a Challenge is provided.

60475639 . 060403

Card Application Related Data - M/Chip 2.1
Transaction Related Terminal Data

B

Card Application Related Data - M/Chip 2.1

This appendix provides a formal definition of all data elements that need be personalized with a M/Chip 2.1 compliant ICC Application.

Card Application Related Data - M/Chip 2.1

Introduction	1
Card Application Personalisation Profile	1
AC Master Key	1
Application Control (9F60)	1
Application Currency Code (9F42)	1
Application Currency Exponent (9F44)	1
Application Effective Date (5F25)	2
Application Expiration Date (5F24)	2
Application File Locator / AFL (94)	2
Application Identifier / AID	2
Application Interchange Profile (82)	2
Application Label (50)	2
Application PAN Sequence Number (5F34)	3
Application Preferred Name (9F12)	3
Application Primary Account Number / PAN (5A)	3
Application Priority Indicator (87)	3
Application Usage Control (9F07)	3
Application Version Number (9F08)	3
Card Issuer Action Code - Decline (C3)	3
Card Issuer Action Code - Offline (C4)	4
Card Issuer Action Code - Online (C5)	4
Card Risk Management Data Object List 1 / CDOL1 (8C)	4
Card Risk Management Data Object List 2 / CDOL2 (8D)	5
Cardholder Name (5F20)	5
Cardholder Name Extended (5F0B)	5
Cardholder Verification Method List / CVM (8E)	6
Certification Authority Public Key Index (8F)	6
Dynamic Data Authentication Data Object List / DDOL (9F49)	6
File Control Information / FCI	6
ICC Dynamic Number Master Key	6
ICC PIN Encipherment Private Key	6
ICC PIN Encipherment Public Key Certificate (9F2D)	7
ICC PIN Encipherment Public Key Exponent (9F2E)	7
ICC PIN Encipherment Public Key Remainder (9F2F)	7
ICC Private Key	7
ICC Public Key Certificate (9F46)	7
ICC Public Key Remainder (9F48)	7
Issuer Action Code - Default (9F0D)	8

Card Application Related Data - M/Chip 2.1

Issuer Action Code - Denial (9F0E)	8
Issuer Action Code - Online (9F0F)	8
Issuer Code Table Index (9F11)	8
Issuer Country Code (5F28)	8
Issuer Internet Proprietary Bitmap / IIPB (9F56)	8
Issuer Public Key Certificate (90)	9
Issuer Public Key Exponent (9F32)	9
Issuer Public Key Remainder (92)	9
Key Derivation Index	9
Language Preference (5F2D)	9
Length of ICC Public Key Modulus	9
Length of PIN Encipherment Public Key Modulus	10
Lower Consecutive Offline Limit (9F14)	10
Lower Cumulative Offline Transaction Amount (CA)	10
Maximum Domestic Offline Transaction Amount (C2)	10
PIN Try Limit / PTL	10
Processing Options Data Object List / PDOL (9F38)	10
Reference Currency Conversion Table (D1)	11
Reference PIN	11
SDA Tag List (9F4A)	11
Service Code (5F30)	11
Signed Static Application Data (93)	11
Track-1 Discretionary Data (9F1F)	11
Track-2 Discretionary Data (9F20)	11
Track-2 Equivalent Data (57)	12
Upper Consecutive Offline Limit (9F23)	12
Upper Cumulative Offline Transaction Amount (CB)	12
Application Cryptogram Calculation	12
Generating the SecureCode™	15

Introduction

The tables in this appendix provide formal definitions for all data object that need be personalized in a M/Chip 2.1 compliant ICC Application used for the MasterCard Chip Authentication service.

For details on the meaning and encoding specifications of the data elements, the reader is referred to the related EMV specification documents:

EMV2000 Integrated Circuit Card Specifications for Payment Systems - Book 3,
Application Specification; Version 4.0 - December, 2000.

Card Application Personalisation Profile

AC Master Key

The Card's master key used for the calculation must be shared between the card and the entity / entities that validate the cryptogram. MasterCard recommends the AC Master Key is a key that is derived from an Issuer Master Key (IMK), using the Application PAN and the Application PAN Sequence number as the data elements used for the key derivation.

Note that it is a MasterCard security policy that two applications sharing the same card, here the payment application and the application used for the Chip Authentication, should NOT share the same Issuer Master Key.

Application Control (9F60)

Since no script commands will be used for the Chip Authentication Application and the transaction will be terminated by the terminal requesting for an AAC, the Application Control may be set to '00'.

Application Currency Code (9F42)

The Chip Authentication Application does not use this information. The field may be personalised on the card, if needed, with any value except for '0999'.

Application Currency Exponent (9F44)

The Chip Authentication Application does not use this information. The field may be personalised on the card, if needed, with a zero value.

Application Effective Date (5F25)

The Chip Authentication Application does not use this information. The field may be personalised on the card, if needed, with any valid date value.

Application Expiration Date (5F24)

The Chip Authentication Application does not use this information. The field may be personalised on the card, if needed, with any valid date value.

Application File Locator / AFL (94)

The AFL indicates to the terminal application what records must be read and also what records contain signed static data for use in the Offline CAM. The value of the AFL should reflect the file structure that is personalised in the card application but because the terminal application used for Chip Authentication will not perform Offline CAM, records containing the Public Key certificates do not need to be identified in the AFL, for the same reason the fourth byte of each AFL entry (the one indicating the number of records to include in the CAM) can be set to '00'.

Application Identifier / AID

The value of the AID must match the value of the DF Name in the FCI. The value of the AID is specified by MasterCard and must be set to **0xA000000048002**.

Application Interchange Profile (82)

The value of the Application Interchange Profile personalised with the M/Chip 2.1 application used for the Chip Authentication can be set to '1000' (Only the bit corresponding to "Cardholder Verification is supported" is set).

Application Label (50)

The terminal application used for the MasterCard Authentication service will not enter into a dialogue with the Cardholder during the Application Selection processing; the data element Application Label can therefore be omitted from the data elements personalized on the card application.

60475639 . 060403

Card Application Related Data - M/Chip 2.1
Card Application Personalisation Profile

Application PAN Sequence Number (5F34)

The Chip Authentication Application does not use this information. MasterCard however recommends it is personalised with the PAN Sequence Number associated with the card for use with connected card readers - if needed.

Application Preferred Name (9F12)

The terminal application used for the MasterCard Authentication service will not enter into a dialogue with the Cardholder during the Application Selection processing; the data element Application Preferred Name can therefore be omitted from the data elements personalized on the card application.

Application Primary Account Number / PAN (5A)

The Chip Authentication Application does not use this information. MasterCard however recommends it is personalised with the PAN associated with the card for use with connected card readers - if needed.

Application Priority Indicator (87)

The terminal application used for the MasterCard Authentication service will not establish a list of mutually supported applications and ignore the bit indicating the application can only be selected after Cardholder confirmation.; the data element Application Priority Indicator can therefore be omitted from the data elements personalized on the card application or be personalized with a value set to '00'.

Application Usage Control (9F07)

The Chip Authentication Application does not use this information. The field may be personalised on the card, if needed, with all bits set to '0'.

Application Version Number (9F08)

The Chip Authentication Application does not use this information. If present on the card MasterCard requires it is personalised with the Application Version Number set to '02'.

Card Issuer Action Code - Decline (C3)

This MasterCard proprietary data element should be personalized with bits corresponding to the following conditions set:

Card Application Related Data - M/Chip 2.1
Card Application Personalisation Profile

- Offline PIN Verification failed.
- PIN Try Limit Exceeded.
- Application blocked by card because PIN Try Limit exceeded.

The resulting Card Issuer Action Code - Decline value to be personalized in the Card Application is '024200'.

Card Issuer Action Code - Offline (C4)

Since the terminal application used for the Authentication service will not ask for an offline approval, this MasterCard proprietary data element will be ignored by the M/Chip 2.1 compliant Card Application.

The Card Issuer Action Code - Offline value to be personalized in the Card Application is therefore '000000'.

Card Issuer Action Code - Online (C5)

Since the terminal application used for the Authentication service will always ask for an online request, this MasterCard proprietary data element will be ignored by the M/Chip 2.1 compliant Card Application.

The Card Issuer Action Code - Online value to be personalized in the Card Application is therefore '000000'.

Card Risk Management Data Object List 1 / CDOL1 (8C)

This data element is to be personalised for use by the terminal application involved with chip authentication. For a M/Chip 2.1 compliant application the CDOL1 must be set to '9F0206' || '9F0306' || '9F1A02' || '9505' || '5F2A02' || '9A03' || '9C01' || '9F3704' || '9F3501' || '9F3A06' || '9F3C02' || '9F4C08⁸' || '9F4502'.

⁸ This data element is not provided for a M/Chip Lite 2.1 Card Application

60475639 060403

Card Application Related Data - M/Chip 2.1

Card Application Personalisation Profile

The contents of the CDOL1 correspond to the concatenated tag and length for the following data elements:

- Amount, Authorised (9F02)
- Amount, Other (9F03)
- Terminal Country Code (9F1A)
- Terminal Verification Result / TVR (95)
- Transaction Currency Code (5F2A)
- Transaction Date (9A)
- Transaction Type (9C)
- Unpredictable Number (9F37)
- Terminal Type (9F35)
- Amount in Reference Currency (9F3A)
- Transaction Reference Currency Code (9F3C)
- ICC Dynamic Number (9F4C)⁹
- Data Authentication Code (9F45)

Card Risk Management Data Object List 2 / CDOL2 (8D)

This data element is to be personalised for use by the terminal application involved with chip authentication. For a M/Chip 2.1 compliant application the CDOL2 must be set to '910A' || '8A02' || '9505' || '9F3704'¹⁰.

The contents of the CDOL2 correspond to the concatenated tag and length for the following data elements:

- Issuer Authentication Data (91)
- Authorisation Response Code (8A)
- Terminal Verification Result / TVR (95)
- Unpredictable Number (9F37)¹¹

Cardholder Name (5F20)

The Chip Authentication Application does not use this information. The field may be personalised on the card, if needed, with a value of all spaces.

Cardholder Name Extended (5F0B)

The Chip Authentication Application does not use this information. The field may be personalised on the card, if needed, with a value of all spaces.

⁹ This data element is not provided for a M/Chip Lite 2.1 Card Application

¹⁰ This data element is not provided for a M/Chip Lite 2.1 Card Application

¹¹ This data element is not provided for a M/Chip Lite 2.1 Card Application

Card Application Related Data - M/Chip 2.1
Card Application Personalisation Profile

Cardholder Verification Method List / CVM (8E)

The Chip Authentication Application only supports one Cardholder Verification Method, the Cleartext PIN verified by the ICC. The data element must therefore be personalised with the following value: '00000000' || '00000000' || '0101' ('X' amount set to '0', 'Y' amount set to '0' and always perform Cleartext PIN verified by the ICC).

Certification Authority Public Key Index (8F)

The Chip Authentication Application does not involve offline Card Authentication; the data element Certification Authority Public Key Index will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

Dynamic Data Authentication Data Object List / DDOL (9F49)

The Chip Authentication Application does not involve offline Card Authentication; the data element Dynamic Data Authentication Data Object List will therefore not be used. If needed because of constraints imposed by the personalisation system, the field must be set to '9F3704' (Unpredictable Number).

File Control Information / FCI

There are no specific requirements for the personalisation of the FCI. Note that M/Chip 2.1 does NOT use a PDOL; the entry must therefore not be present in the File Control Information.

ICC Dynamic Number Master Key

The Chip Authentication does not involve offline CAM; this data element is therefore not needed and may be personalized with any value.

ICC PIN Encipherment Private Key

The Chip Authentication Application does not involve offline Card Authentication and does not support Enciphered PIN as a valid offline CVM; the data element PIN Encipherment Private Key will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

ICC PIN Encipherment Public Key Certificate (9F2D)

The Chip Authentication Application does not involve offline Card Authentication and does not support Enciphered PIN as a valid offline CVM; the data element ICC PIN Encipherment Public Key Certificate will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

ICC PIN Encipherment Public Key Exponent (9F2E)

The Chip Authentication Application does not involve offline Card Authentication and does not support Enciphered PIN as a valid offline CVM; the data element ICC PIN Encipherment Public Key Exponent will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

ICC PIN Encipherment Public Key Remainder (9F2F)

The Chip Authentication Application does not involve offline Card Authentication and does not support Enciphered PIN as a valid offline CVM; the data element ICC PIN Encipherment Public Key Remainder will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

ICC Private Key

The Chip Authentication Application does not involve offline Card Authentication; the data element ICC Private Key will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

ICC Public Key Certificate (9F46)

The Chip Authentication Application does not involve offline Card Authentication; the data element ICC Public Key Certificate will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

ICC Public Key Remainder (9F48)

The Chip Authentication Application does not involve offline Card Authentication; the data element ICC Public Key Remainder will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

Card Application Related Data - M/Chip 2.1
Card Application Personalisation Profile

Issuer Action Code - Default (9F0D)

Issuer Action Codes are not used by the terminal application involved with the Chip Authentication to decide on the type of cryptogram they request from the card. The field may be personalised on the card, if needed, with all bits set to '0'.

Issuer Action Code - Denial (9F0E)

Issuer Action Codes are not used by the terminal application involved with the Chip Authentication to decide on the type of cryptogram they request from the card. The field may be personalised on the card, if needed, with all bits set to '0'.

Issuer Action Code - Online (9F0F)

Issuer Action Codes are not used by the terminal application involved with the Chip Authentication to decide on the type of cryptogram they request from the card. The field may be personalised on the card, if needed, with all bits set to '0'.

Issuer Code Table Index (9F11)

The Chip Authentication Application does not use the data element Issuer Code Table Index. The field may therefore be personalised with any value that matches the edit rules, if needed.

Issuer Country Code (5F28)

The Chip Authentication Application does not use this information. The field may be personalised on the card, if needed, with any valid country code or '0000'.

Issuer Internet Proprietary Bitmap / IIPB (9F56)

A bitmap used by the terminal application to identify the bits from the data generated by the Card Application that must be used to build the Authentication Token.

The IIPB is laid over the concatenated data elements:

1. Cryptogram Information Data.
2. Application Transaction Counter
3. Application Cryptogram
4. Issuer Application Data / Key Derivation Index.
5. Issuer Application Data / Cryptogram Version Number.
6. Issuer Application Data / Card Verification Results.

Card Application Related Data - M/Chip 2.1
Card Application Personalisation Profile

For a M/Chip 2.1 Compliant Application as specified in this paper, the IIPB can be set to the following value: '00' || '0OFF' || '00000000FFFFFF' || '00' || '00' || '00200000'.

Issuer Public Key Certificate (90)

The Chip Authentication Application does not involve offline Card Authentication; the data element Issuer Public Key Certificate will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

Issuer Public Key Exponent (9F32)

The Chip Authentication Application does not involve offline Card Authentication; the data element Issuer Public Key Exponent will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

Issuer Public Key Remainder (92)

The Chip Authentication Application does not involve offline Card Authentication; the data element Issuer Public Key Remainder will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

Key Derivation Index

Card Issuers that use a Key Derivation Index to identify the Issuer Master Key (IMK) to be used for the AC Master Key derivation may personalize this value; the Key Derivation Index will be inserted in the Issuer Application Data returned by the card in its response to a GENERATE AC command.

Language Preference (5F2D)

The Chip Authentication Application does not use this information. The field may be personalised on the card, if needed, with a value of all spaces.

Length of ICC Public Key Modulus

The Chip Authentication Application does not involve offline Card Authentication; the data element Length of ICC Public Key Modulus will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any

Card Application Related Data - M/Chip 2.1
Card Application Personalisation Profile

valid value.

Note the data element is not to be personalised with a 'Lite' profile.

Length of PIN Encipherment Public Key Modulus

The Chip Authentication Application does not involve offline Card Authentication and does not support Enciphered PIN as a valid offline CVM; the data element Length of PIN Encipherment Public Key Modulus will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

Lower Consecutive Offline Limit (9F14)

To allow for predictable Card Verification Results (CVR) settings, the Lower Consecutive Offline Limit should be set to '00', as a result the limit will always be exceeded.

Lower Cumulative Offline Transaction Amount (CA)

To allow for predictable Card Verification Results (CVR) settings, the Lower Cumulative Offline Transaction Amount should be set to '000000000000', as a result the limit will always be exceeded.

Maximum Domestic Offline Transaction Amount (C2)

To allow for predictable Card Verification Results (CVR) settings, the Maximum Domestic Offline Transaction Amount should be set to '999999999999', as a result the limit will never be exceeded.

PIN Try Limit / PTL

The PIN Try Limit for the Card Application used for the Chip Authentication should be set to '03'.

Processing Options Data Object List / PDOL (9F38)

The Chip Authentication Application does not use the data element Processing Options Data Object List / PDOL; the field is therefore NOT to be personalised.

Reference Currency Conversion Table (D1)

The Chip Authentication Application does not use the data element Reference Currency Conversion Table. The field may therefore be personalised with any value - including a zero length - that matches the edit rules, if needed.

Reference PIN

The data element Reference PIN must be personalized with the value of the Offline PIN used for the Authentication Service. MasterCard recommends the Offline PIN is shared with the other payment applications loaded on the ICC and is set to the same value as the online PIN.

SDA Tag List (9F4A)

The Chip Authentication Application does not involve offline Card Authentication; the data element SDA Tag list will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

Service Code (5F30)

The Chip Authentication Application does not use the data element Service Code. The field may therefore be personalised with any value that matches the edit rules, if needed.

Signed Static Application Data (93)

The Chip Authentication Application does not involve offline Card Authentication; the data element Signed Static Application Data will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

Track-1 Discretionary Data (9F1F)

The Chip Authentication Application does not use the data element Track-1 Discretionary Data. The field may therefore be personalised with any value that matches the edit rules, if needed.

Track-2 Discretionary Data (9F20)

The Chip Authentication Application does not use the data element Track-2 Discretionary Data. The field may therefore be personalised with any value that matches the edit rules, if needed.

Card Application Related Data - M/Chip 2.1
Application Cryptogram Calculation

Track-2 Equivalent Data (57)

Terminal applications involved with Chip Authentication will not read the electronic version of the Track-2 from the chip; the data element may therefore be omitted from the data personalised on the card or filled with any value that satisfies the specifications for the field.

Upper Consecutive Offline Limit (9F23)

To allow for predictable Card Verification Results (CVR) settings, the Upper Consecutive Offline Limit should be set to '00', as a result the limit will always be exceeded.

Upper Cumulative Offline Transaction Amount (CB)

To allow for predictable Card Verification Results (CVR) settings, the Upper Cumulative Offline Transaction Amount should be set to '000000000000', as a result the limit will always be exceeded.

Application Cryptogram Calculation

Disclaimer: The MasterCard M/Chip 2.1 Card Application Specification do not specify its behaviour when 2 or more instances of the application are implemented on the same chip. It therefore is difficult to say if Card Risk Management counters, Script Counters, ... are maintained on a per AID bases or that they are shared between the different applications. For the sake of this feasibility study we assume data is isolated; the only exception is the Offline PIN which we assume to be shared.

All transaction related data elements originating from the terminal are predictable for the Card Issuer's validation systems; the only exception is the 'Unpredictable Number' field that can be used to link the Authentication Token to a specific transaction / event.

- Amount, Authorised.
- Amount, Other.
- Terminal Country Code.
- Terminal Verification Results.
- Transaction Currency Code.
- Transaction Date.
- Transaction Type.
- Unpredictable Number.
- Application Interchange Profile.

Card Application Related Data - M/Chip 2.1
Application Cryptogram Calculation

The M/Chip 2.1 card application used for authentication purposes is personalised to minimize the data included in the cryptogram calculation; the Application Control field will therefore be set not to include the offline risk management counters (Cumulative Offline Transaction Amount and Consecutive Offline Transaction Number).

Therefore remains the Card related data included in the Cryptogram calculation:

- Application Transaction Counter.
- Card Verification Results.

The Application Transaction Counter field is a 2 byte binary counter that is incremented each time the card application processes the 'Get Processing Option' sequence.

While we can envisage truncating part of the counter and only carry the least significant bits, one must be aware that Card Application developers may develop the M/Chip 2.1 application such that multiple instances of the application share the same Application Transaction Counter or each have their own counter.

The Card Verification Result is a 4 byte bitmap that indicates processing status on the current transaction and on the previous transaction(s). We assume that multiple instances of the M/Chip 2.1 application will not share the TVR information i.e. Script processing information in the 'Payment' application will not be reflected in the 'Authentication' application.

Byte	Bit	Meaning	Carry
1	8	Set to '0' - Byte value set to '03'.	
	7	Set to '0'	
	6	Set to '0'	
	5	Set to '0'	
	4	Set to '0'	
	3	Set to '0'	
	2	Set to '1'	
	1	Set to '1'	
2	8	Together with the next bit this encodes the Type of Application Cryptogram returned in the second Generate AC. For the first Generate AC we assume these bits are set to '10' (Cryptogram not requested yet).	
	7	See bit 8.	
	6	Together with the next bit this encodes the Type of Application Cryptogram returned in the first Generate AC. Since the Card Application will only return an ARQC ('10') or AAC ('00') cryptogram, it will be sufficient to carry this first bit - the value of the second bit is redundant.	x
	5	See bit 6.	
	4	Issuer Authentication failed. Since the Authentication Terminal will not get the response from the	

Card Application Related Data - M/Chip 2.1
Application Cryptogram Calculation

Byte	Bit	Meaning	Carry
		Card Issuer, we can assume the bit will be set to '0'	
	3	Offline PIN Verification Performed. We can assume this bit will always be set to '1' indicating the CVM was performed.	
	2	Offline PIN Verification Failed. We can assume PIN Verification was Successful (bit set to '0') and not carry the information.	
	1	Unable to go online. For a First Generate AC the bit will be set to '0'.	
3	8	Last Online Transaction Not Completed. We can assume this bit will be set to '1'.	
	7	PTL Exceeded. We can assume this bit set to '0' (PTL Not exceeded).	
	6	Exceeds Velocity Checking. Setting of the limits will be such that the bit will be set to '1'.	
	5	New Card. One can assume this bit is set to '0'	
	4	Issuer Authentication Failed. We can assume this bit was / is set to '1' (Issuer Authentication Failed).	
	3	Issuer Authentication not performed after online authorisation. We can assume this bit was / is set to '1' (Issuer Authentication Not Performed).	
	2	Application blocked by card because PIN Try Limit exceeded. We can assume this bit was / is set to '0'	
	1	Static data authentication failed on last transaction and transaction declined offline. Must be set to '0'	
4	8	Together with the following bits this contains the count of the Number of Script Commands processed successfully. We can assume this count is always '000' or known to Card Issuer.	
	7	See bit 8.	
	6	See bit 8.	
	5	DDA failed on last online transaction and transaction declined offline. ¹² DDA is not performed - Bit value set to '0'.	
	4	Issuer script processing failed on last or current transaction. We can assume this count is always '0' or known to Card Issuer.	
	3	Lower Consecutive Offline Limit or Lower Cumulative Offline Transaction Amount exceeded. Because of the values personalized in the Card Application, we can	

¹² This bit is always set to '0' for a M/Chip Lite Card Application.

Card Application Related Data - M/Chip 2.1
Generating the SecureCode(

Byte	Bit	Meaning	Carry
		assume this bit is set to '1'.	
	2	Upper Consecutive Offline Limit or Upper Cumulative Offline Transaction Amount exceeded. Because of the values personalized in the Card Application, we can assume this bit is set to '1'.	
	1	Maximum Offline transaction Amount exceeded. ¹³ Because of the values personalized in the Card Application, we can assume this bit is set to '0'.	

Generating the SecureCode™

The Response Message returned by the M/Chip Card Application contains the following Data:

- Cryptogram Information Data.
- Application Transaction Counter
- Application Cryptogram
- Issuer Application Data / Key Derivation Index.
- Issuer Application Data / Cryptogram Version Number.
- Issuer Application Data / Card Verification Results.
- Issuer Application Data / DAC or ICC Dynamic Number.

The Cryptogram Information Data does not need to be carried; the information is redundant with the status information in the CVR; Card Issuers can assume its value is '80' (i.e. the value indicating the Card Application returned an ARQC).

The Application Transaction Counter is needed for the Session Key Derivation; we can however carry a shorter value of the ATC and rebuild the full value at the Card Issuer side. We propose to carry 8 bits, this allows for 256 Cryptogram calculations without the Card Issuer being unable to validate the cryptogram.

The Application Cryptogram must be carried but we can shorten the information carried and have the Card Issuer to compare a portion of the calculated cryptogram with the information carried in the request. We propose to carry 16 bits; this should give sufficient confidence the Cryptogram calculated by the Card Issuer matches the Cryptogram generated by the Card Application.

The Key Derivation Index does not need to be carried - Card Issuers know what Card key derivation method is used for their cards and can find shortcuts that do not require this data element at Cryptogram Validation time.

¹³ This bit is always set to '0' for a M/Chip Lite Card Application.

Card Application Related Data - M/Chip 2.1
Generating the SecureCode(

The Cryptogram Version Number does not to be carried - Card Issuers know what session key derivation method is used for their card and therefore do not need to carry the information.

We do not need to carry the full value of the Card Verification Results; as shown in the table we only need to carry 1 bit.

The DAC included in the response is the same value provided by the Authentication Terminal; it therefore can be set to '0' and does not to be carried (it is not included in the Cryptogram Calculation either).

The Authentication Token is build by the terminal application; to make the application generic, MasterCard recommends the use of the Issuer Internet Proprietary Bitmap / IIPB data element to identify what bit values to select for the generation of the Authentication token.

60475639 . 060403

Card Application Related Data - M/Chip 4
Generating the SecureCode(

C

Card Application Related Data - M/Chip 4

This appendix provides a formal definition of all data elements that need be personalized with a M/Chip 4 compliant ICC Application.

Introduction	1
Card Application Personalisation Profile	1
AC Master Key.....	1
Additional Check Table (D3).....	1
Application Control (D5).....	1
Application Currency Code (9F42).....	2
Application Effective Date (5F25).....	2
Application Expiration Date (5F24).....	2
Application File Locator / AFL (94).....	2
Application Identifier / AID	2
Application Interchange Profile (82).....	2
Application Life Cycle Data (9F7E).....	2
Application PAN Sequence Number (5F34)	3
Application Primary Account Number / PAN (5A)	3
Application Usage Control (9F07).....	3
Application Version Number (9F08)	3
Card Issuer Action Code / CIAC - Decline (C3).....	3
Card Issuer Action Code / CIAC - Default (C4).....	3
Card Issuer Action Code / CIAC - Online (C5)	3
Card Risk Management / CRM - Country Code (C8).....	4
Card Risk Management / CRM - Currency Code (C9)	4
Card Risk Management Data Object List 1 / CDOL1 (8C)	4
Card Risk Management Data Object List 2 / CDOL2 (8D).....	5
Cardholder Name (5F20)	5
Cardholder Verification Method List / CVM (8E).....	5
CDOL1 Related Data Length (C7).....	5
Certification Authority Public Key Index (8F)	5
CFDC - Limit for AC Session Key.....	6
CFDC - Limit for Confidentiality Session Key	6
CFDC - Limit for Integrity Session Key.....	6
Currency Conversion Table (D1).....	6
Default ARPC Response Code (D6)	6
Dynamic Data Authentication Data Object List / DDOL (9F49)	6
File Control Information / FCI	7
ICC Dynamic Number Master Key.....	7
IOC PIN Encipherment Private Key	7
IOC PIN Encipherment Public Key Certificate (9F2D)	7
IOC PIN Encipherment Public Key Exponent (9F2E)	7

Card Application Related Data - M/Chip 4

ICC PIN Encipherment Public Key Remainder (9F2F)	7
ICC Private Key.....	8
ICC Public Key Certificate (9F46)	8
ICC Public Key Remainder (9F48)	8
Issuer Action Code - Default (9F0D).....	8
Issuer Action Code - Denial (9F0E).....	8
Issuer Action Code - Online (9F0F).....	8
Issuer Country Code (5F28).....	9
Issuer Internet Proprietary Bitmap / IIPB (9F56)	9
Issuer Public Key Certificate (90).....	9
Issuer Public Key Exponent (9F32).....	9
Issuer Public Key Remainder (92).....	9
Key Derivation Index.....	10
Length of ICC Public Key Modulus	10
Length of PIN Encipherment Public Key Modulus	10
Lower Consecutive Offline Limit (9F14).....	10
Lower Cumulative Offline Transaction Amount (CA).....	10
PIN Try Limit / PTL	10
SDA Tag List (9F4A)	11
Signed Static Application Data (93)	11
SM For Confidentiality Master Key.....	11
SM For Integrity Master Key.....	11
Track-2 Equivalent Data (57).....	11
Upper Consecutive Offline Limit (9F23).....	11
Upper Cumulative Offline Transaction Amount (CB)	11
Application Cryptogram Calculation.....	12
Generating the Authentication Token	15

Introduction

The tables in this appendix provide formal definitions for all data object that need be personalized in a M/Chip 4 compliant ICC Application used for the MasterCard Chip Authentication service.

For details on the meaning and encoding specifications of the data elements, the reader is referred to the related EMV specification documents:

EMV2000 Integrated Circuit Card Specifications for Payment Systems - Book 3,
Application Specification; Version 4.0 - December, 2000.

Card Application Personalisation Profile

AC Master Key

The Card's master key used for the calculation must be shared between the card and the entity / entities that validate the cryptogram. MasterCard recommends the AC Master Key is a key that is derived from an Issuer Master Key (IMK), using the Application PAN and the Application PAN Sequence number as the data elements used for the key derivation.

Note that it is a MasterCard security policy that two applications sharing the same card, here the payment application and the application used for the Chip Authentication, should NOT share the same Issuer Master Key.

Additional Check Table (D3)

The Additional Checks will not be used for the Chip Authentication. If the data element Additional Check Table must be personalised on the Card Application then its value should be set to '000000FFFF...FFFF'.

Application Control (D5)

This data element should be set to b'000001x0' || b'00000000'; this corresponds to the following settings:

- Magstripe Issuer not activated.
- Do not skip CIAC Default on CAT3.
- Offline plaintext PIN verification supported.
- Session Key derivation is left to the discretion of the Card Issuer (must be specified before personalisation).
- Do not encrypt offline counters.
- Do not activate additional check table.
- Do not include counters in Application Cryptogram calculation.

Card Application Related Data - M/Chip 4
Card Application Personalisation Profile

Application Currency Code (9F42)

The Chip Authentication Application does not use this information. The field may be personalised on the card, if needed, with any value except for '0999'.

Application Effective Date (5F25)

The Chip Authentication Application does not use this information. The field may be personalised on the card, if needed, with any valid date value.

Application Expiration Date (5F24)

The Chip Authentication Application does not use this information. The field may be personalised on the card, if needed, with any valid date value.

Application File Locator / AFL (94)

The AFL indicates to the terminal application what records must be read and also what records contain signed static data for use in the Offline CAM. The value of the AFL should reflect the file structure that is personalised in the card application but because the terminal application used for Chip Authentication will not perform Offline CAM, records containing the Public Key certificates do not need to be identified in the AFL, for the same reason the fourth byte of each AFL entry (the one indicating the number of records to include in the CAM) can be set to '00'.

Application Identifier / AID

The value of the AID must match the value of the DF Name in the FCI. The value of the AID is specified by MasterCard and must be set to **0xA000000048002**.

Application Interchange Profile (82)

The value of the Application Interchange Profile personalised with the M/Chip 4 application used for the Chip Authentication can be set to '1000' (Only the bit corresponding to "Cardholder Verification is supported" is set).

Application Life Cycle Data (9F7E)

The Application Life Cycle Data will need to be personalised with the right values for the Version Number, Type Approval Identification Code, Application Issuer Identification and Application Code Identification.

60475639 . 060403

Card Application Related Data - M/Chip 4
Card Application Personalisation Profile

Application PAN Sequence Number (5F34)

The Chip Authentication Application does not use this information. MasterCard however recommends it is personalised with the PAN Sequence Number associated with the card for use with connected card readers - if needed.

Application Primary Account Number / PAN (5A)

The Chip Authentication Application does not use this information. MasterCard however recommends it is personalised with the PAN associated with the card for use with connected card readers - if needed.

Application Usage Control (9F07)

The Chip Authentication Application does not use this information. The field may be personalised on the card, if needed, with all bits set to '0'.

Application Version Number (9F08)

The Chip Authentication Application does not use this information. If present on the card MasterCard requires it is personalised with the Application Version Number set to '02'.

Card Issuer Action Code / CIAC - Decline (C3)

The Card Issuer Action Code /CIAC - Decline used for the Card Application involved with the Chip Authentication should be set to '390000'. These settings indicate always to generate an AAC if one or more of the following conditions are satisfied:

- Offline PIN not performed.
- Offline PIN Verification Failed.
- PTL Exceeded.
- Terminal erroneously considers Offline PIN OK.

Card Issuer Action Code / CIAC - Default (C4)

The Card Issuer Action Code /CIAC - Default used for the Card Application involved with the Chip Authentication should be set to '000000'.

Card Issuer Action Code / CIAC - Online (C5)

The Card Issuer Action Code /CIAC - Online used for the Card Application involved with the Chip Authentication should be set to '000000'.

Card Application Related Data - M/Chip 4**Card Application Personalisation Profile****Card Risk Management /CRM - Country Code (C8)**

The Card Application is not expected to perform Card Risk Management; the Card Risk Management /CRM - Country Code can therefore be set to '0000'.

Card Risk Management /CRM - Currency Code (C9)

To avoid interference between the terminal application involved with Chip Authentication and the Card Application's Offline Risk Management, the Card Risk Management /CRM - Currency Code should be personalised with a value set to '9999'¹⁴.

Card Risk Management Data Object List 1 / CDOL1 (8C)

This data element is to be personalised for use by the terminal application involved with chip authentication. For a M/Chip 4 compliant application the CDOL1 must be set to '9F0206' || '9F0306' || '9F1A02' || '9505' || '5F2A02' || '9A03' || '9C01' || '9F3704' || '9F3704' || '9F3501' || '9F4502' || '9F4C08¹⁵' || '9F3403'.

The total length of the CDOL1 data must match the length personalised in the proprietary data element CDOL1 Related Data Length (C7).

The contents of the CDOL1 correspond to the concatenated tag and length for the following data elements:

- Amount, Authorised (9F02)
- Amount, Other (9F03)
- Terminal Country Code (9F1A)
- Terminal Verification Result / TVR (95)
- Transaction Currency Code (5F2A)
- Transaction Date (9A)
- Transaction Type (9C)
- Unpredictable Number (9F37)
- Terminal Type (9F35)
- Data Authentication Code (9F45)
- ICC Dynamic Number (9F4C)
- CVM Results (9F34)

¹⁴ We use the value '9999' as a filler; this avoids confusion when the terminal returns '0000' as the transaction currency ('0000' indicates information is not available)

¹⁵ Note this data element is not included in the CDOL personalised for a M/Chip 4 'Lite' profile.

Card Risk Management Data Object List 2 / CDOL2 (8D)

This data element is to be personalised for use by the terminal application involved with chip authentication. For a M/Chip 4 compliant application the CDOL2 must be set to '910A' || '8A02' || '9505' || '9F3704' || '9F4C08'¹⁶.

The contents of the CDOL2 correspond to the concatenated tag and length for the following data elements:

- Issuer Authentication Data (91)
- Authorisation Response Code (8A)
- Terminal Verification Result / TVR (95)
- Unpredictable Number (9F37)
- ICC Dynamic Number (9F4C)

Cardholder Name (5F20)

The Chip Authentication Application does not use this information. The field may be personalised on the card, if needed, with a value of all spaces.

Cardholder Verification Method List / CVM (8E)

The Chip Authentication Application only supports one Cardholder Verification Method, the Cleartext PIN verified by the IOC. The data element must therefore be personalised with the following value: '00000000' || '00000000' || '0101' ('X' amount set to '0', 'Y' amount set to '0' and always perform Cleartext PIN verified by the IOC).

CDOL1 Related Data Length (C7)

This data element must be personalised to the length of the data expected to be included by the terminal in the GENERATE AC command. It must match the sum of the individual lengths specified for the tags included in the CDOL1.

Certification Authority Public Key Index (8F)

The Chip Authentication Application does not involve offline Card Authentication; the data element Certification Authority Public Key Index will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

¹⁶ Note this data element is not included in the CDOL personalised for a M/Chip 4 'Lite' profile.

Card Application Related Data - M/Chip 4**Card Application Personalisation Profile****CFDC - Limit for AC Session Key**

This security parameter is needed if the Card Application is configured to use the EMV 2000 Session key derivation algorithm; if applicable it should be set to '03'.

CFDC - Limit for Confidentiality Session Key

The Chip Authentication does not involve script processing; this data element is therefore not needed and may be personalized with any value.

CFDC - Limit for Integrity Session Key

The Chip Authentication does not involve script processing; this data element is therefore not needed and may be personalized with any value.

Currency Conversion Table (D1)

The Chip Authentication will not involve currency conversion; the table must therefore be initialized with the filler value '9999000000' || '9999000000' || '9999000000' || '9999000000' || '9999000000'.¹⁷

Default ARPC Response Code (D6)

Since we did not activate the Magstripe Issuer profile in the Application Control, the Default ARPC Response Code will not be used. If needed for compatibility with the Payment Application, the value of the Default ARPC Response Code should be set to '03' (PTC re-initialized to '3').

Dynamic Data Authentication Data Object List / DDOL (9F49)

The Chip Authentication Application does not involve offline Card Authentication; the data element Dynamic Data Authentication Data Object List will therefore not be used. If needed because of constraints imposed by the personalisation system, the field must be set to '9F3704' (Unpredictable Number).

¹⁷ We use the value '9999' as a filler for the currency code to avoid confusion when the terminal returns '0000' as the transaction currency ('0000' indicates information is not available)

File Control Information / FCI

There are no specific requirements for the personalisation of the FCI. Note that M/Chip 4 does NOT use a PDOL; the entry must therefore not be present in the File Control Information.

ICC Dynamic Number Master Key

The Chip Authentication does not involve offline CAM; this data element is therefore not needed and may be personalized with any value. Note that this data is not personalized for a 'Lite' profile.

ICC PIN Encipherment Private Key

The Chip Authentication Application does not involve offline Card Authentication and does not support Enciphered PIN as a valid offline CVM; the data element PIN Encipherment Private Key will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.
Note the data element is not to be personalized with a 'Lite' profile.

ICC PIN Encipherment Public Key Certificate (9F2D)

The Chip Authentication Application does not involve offline Card Authentication and does not support Enciphered PIN as a valid offline CVM; the data element ICC PIN Encipherment Public Key Certificate will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

ICC PIN Encipherment Public Key Exponent (9F2E)

The Chip Authentication Application does not involve offline Card Authentication and does not support Enciphered PIN as a valid offline CVM; the data element ICC PIN Encipherment Public Key Exponent will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

ICC PIN Encipherment Public Key Remainder (9F2F)

The Chip Authentication Application does not involve offline Card Authentication and does not support Enciphered PIN as a valid offline CVM; the data element ICC PIN Encipherment Public Key Remainder will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

Card Application Related Data - M/Chip 4
Card Application Personalisation Profile

ICC Private Key

The Chip Authentication Application does not involve offline Card Authentication; the data element ICC Private Key will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value. Note the data element is not to be personalized with a 'Lite' profile.

ICC Public Key Certificate (9F46)

The Chip Authentication Application does not involve offline Card Authentication; the data element ICC Public Key Certificate will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

ICC Public Key Remainder (9F48)

The Chip Authentication Application does not involve offline Card Authentication; the data element ICC Public Key Remainder will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

Issuer Action Code - Default (9F0D)

Issuer Action Codes are not used by the terminal application involved with the Chip Authentication to decide on the type of cryptogram they request from the card. The field may be personalised on the card, if needed, with all bits set to '0'.

Issuer Action Code - Denial (9F0E)

Issuer Action Codes are not used by the terminal application involved with the Chip Authentication to decide on the type of cryptogram they request from the card. The field may be personalised on the card, if needed, with all bits set to '0'.

Issuer Action Code - Online (9F0F)

Issuer Action Codes are not used by the terminal application involved with the Chip Authentication to decide on the type of cryptogram they request from the card. The field may be personalised on the card, if needed, with all bits set to '0'.

Issuer Country Code (5F28)

The Chip Authentication Application does not use this information. The field may be personalised on the card, if needed, with any valid country code or '0000'.

Issuer Internet Proprietary Bitmap / IIPB (9F56)

A bitmap used by the terminal application to identify the bits from the data generated by the Card Application that must be used to build the Authentication Token.

The IIPB is laid over the concatenated data elements:

7. Cryptogram Information Data.
8. Application Transaction Counter
9. Application Cryptogram.
10. Issuer Application Data / Key Derivation Index.
11. Issuer Application Data / Cryptogram Version Number.
12. Issuer Application Data / Card Verification Results.

For a M/Chip 4 Compliant Application as specified in this paper, the IIPB can be set to the following value: '00' || '0OFF' || '00000000FFFFFFFFFF' || '00' || '00' || '200000000000'.

Issuer Public Key Certificate (90)

The Chip Authentication Application does not involve offline Card Authentication; the data element Issuer Public Key Certificate will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

Issuer Public Key Exponent (9F32)

The Chip Authentication Application does not involve offline Card Authentication; the data element Issuer Public Key Exponent will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

Issuer Public Key Remainder (92)

The Chip Authentication Application does not involve offline Card Authentication; the data element Issuer Public Key Remainder will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

Card Application Related Data - M/Chip 4
Card Application Personalisation Profile

Key Derivation Index

Card Issuers that use a Key Derivation Index to identify the Issuer Master Key (IMK) to be used for the AC Master Key derivation may personalize this value; the Key Derivation Index will be inserted in the Issuer Application Data returned by the card in its response to a GENERATE AC command.

Length of ICC Public Key Modulus

The Chip Authentication Application does not involve offline Card Authentication; the data element Length of IOC Public Key Modulus will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

Note the data element is not to be personalized with a 'Lite' profile.

Length of PIN Encipherment Public Key Modulus

The Chip Authentication Application does not involve offline Card Authentication and does not support Enciphered PIN as a valid offline CVM; the data element Length of PIN Encipherment Public Key Modulus will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

Note the data element is not to be personalized with a 'Lite' profile.

Lower Consecutive Offline Limit (9F14)

To allow for predictable Card Verification Results (CVR) settings, the Lower Consecutive Offline Limit should be set to '00', as a result the limit will always be exceeded.

Lower Cumulative Offline Transaction Amount (CA)

To allow for predictable Card Verification Results (CVR) settings, the Lower Cumulative Offline Transaction Amount should be set to '999999999999', as a result the limit will never be exceeded.

PIN Try Limit / PTL

The PIN Try Limit for the Card Application used for the Chip Authentication should be set to '03'.

SDA Tag List (9F4A)

The Chip Authentication Application does not involve offline Card Authentication; the data element SDA Tag list will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

Signed Static Application Data (93)

The Chip Authentication Application does not involve offline Card Authentication; the data element Signed Static Application Data will therefore not be used. If needed because of constraints imposed by the personalisation system, the field may be personalised with any valid value.

SM For Confidentiality Master Key

The Chip Authentication does not involve script processing; this data element is therefore not needed and may be personalized with any value.

SM For Integrity Master Key

The Chip Authentication does not involve script processing; this data element is therefore not needed and may be personalized with any value.

Track-2 Equivalent Data (57)

Terminal applications involved with Chip Authentication will not read the electronic version of the Track-2 from the chip; the data element may therefore be omitted from the data personalised on the card or filled with any value that satisfies the specifications for the field.

Upper Consecutive Offline Limit (9F23)

To allow for predictable Card Verification Results (CVR) settings, the Upper Consecutive Offline Limit should be set to '00', as a result the limit will always be exceeded.

Upper Cumulative Offline Transaction Amount (CB)

To allow for predictable Card Verification Results (CVR) settings, the Upper Cumulative Offline Transaction Amount should be set to '999999999999', as a result the limit will never be exceeded.

Application Cryptogram Calculation

Disclaimer: The MasterCard M/Chip 4 Card Application Specification do not specify its behaviour when 2 or more instances of the application are implemented on the same chip. It therefore is difficult to say if Card Risk Management counters, Script Counters, ... are maintained on a per AID bases or that they are shared between the different applications. For the sake of this feasibility study we assume data is isolated; the only exception is the Offline PIN which we assume to be shared.

All transaction related data elements originating from the terminal are predictable for the Card Issuer's validation systems; the only exception is the 'Unpredictable Number' field that can be used to link the Authentication Token to a specific transaction / event.

- Amount, Authorised.
- Amount, Other.
- Terminal Country Code.
- Terminal Verification Results.
- Transaction Currency Code.
- Transaction Date.
- Transaction Type.
- Unpredictable Number.
- Application Interchange Profile.

The M/Chip 4 card application used for authentication purposes is personalised to minimize the data included in the cryptogram calculation; the Application Control field will therefore be set not to include the offline risk management counters (Cumulative Offline Transaction Amount and Consecutive Offline Transaction Number).

Therefore remains the Card related data included in the Cryptogram calculation:

- Application Transaction Counter.
- Card Verification Results.

The Application Transaction Counter field is a 2 byte binary counter that is incremented each time the card application processes the 'Get Processing Option' sequence.

While we can envisage truncating part of the counter and only carry the least significant bits, one must be aware that Card Application developers may develop the M/Chip 4 application such that multiple instances of the application share the same Application Transaction Counter or each have their own counter.

Card Application Related Data - M/Chip 4
Application Cryptogram Calculation

The Card Verification Result is a 6 byte bitmap that indicates processing status on the current transaction and on the previous transaction(s). We assume that multiple instances of the M/Chip 4 application will not share the TVR information i.e. Script processing information in the 'Payment' application will not be reflected in the 'Authentication' application.

Byte	Bit	Meaning	Carry
1	8	Together with the next bit this encodes the Type of Application Cryptogram returned in the second Generate AC. For the first Generate AC we assume these bits are set to '10' (Cryptogram not requested yet).	
	7	See bit 8.	
	6	Together with the next bit this encodes the Type of Application Cryptogram returned in the first Generate AC. Since the Card Application will only return an ARQC ('10') or AAC ('00') cryptogram, it will be sufficient to carry this first bit - the value of the second bit is redundant.	x
	5	See bit 6.	
	4	RFU - Must be set to '0'	
	3	Offline PIN Verification Performed. We can assume this bit will always be set to '1' indicating the CVM was performed.	
	2	Offline Encrypted PIN Verification Performed. We can assume this bit will always be set to '0' indicating this CVM was not performed (the Terminal will not support it).	
	1	Offline PIN Verification Successful. We can assume PIN Verification was Successful (bit set to '1') and not carry the information.	
2	8	DDA Returned. Since the Terminal will not perform offline CAM, the bit will be set to '0'.	
	7	Combined DDA/AC Generation Returned in First Generate AC. Since the Terminal will not perform offline CAM, the bit will be set to '0'.	
	6	Combined DDA/AC Generation Returned in First Generate AC. Since the Terminal will not perform offline CAM, the bit will be set to '0'.	
	5	Issuer Authentication Performed. Since the Authentication Terminal will not get the response from the Card Issuer, we can assume the bit will be set to '0'	
	4	Card Risk Management skipped on CAT3. The Authentication Terminal will not be declared as a CAT3, the bit will therefore always be set to '0'.	
	3	RFU - Must be set to '0'	
	2	RFU - Must be set to '0'	

Card Application Related Data - M/Chip 4

Application Cryptogram Calculation

Byte	Bit	Meaning	Carry
	1	RFU - Must be set to '0'	
3	8	Right nibble of Script Counter. Since we do not send Script Commands to this Card Application, the script counter should remain at '0000'.	
	7	See bit 8.	
	6	See bit 8.	
	5	See bit 8.	
	4	Right nibble of PIN Try Counter. We can assume the PTC is set to '0000' when using the service.	
	3	See bit 4.	
	2	See bit 4.	
	1	See bit 4.	
4	8	RFU - Must be set to '0'	
	7	Unable to go online. This bit is always set to '0' for the first Generate AC.	
	6	Offline PIN Validation not performed. We can assume the bit is set to '0' (PIN Validation is performed).	
	5	Offline PIN Validation Failed. We can assume the bit is set to '0' (No Failure of Offline PIN Validation).	
	4	PTL Exceeded. We can assume this bit set to '0' (PTL Not exceeded).	
	3	International Transaction. We will make sure the Terminal Country Code is always <> from the Issuer Country Code and therefore this bit will always be set.	
	2	Domestic Transaction. We will make sure the Terminal Country Code is always <> from the Issuer Country Code and therefore this bit will always be clear.	
	1	Terminal erroneously considers Offline PIN OK. We can assume the bit is set to '0' (Terminal does not erroneously consider Offline PIN OK).	
5	8	Lower Consecutive Offline Limit Exceeded. We will use a transaction Amount set to 0 and therefore we can assume the bit is set to '0' (Lower Consecutive Offline Limit not Exceeded).	
	7	Upper Consecutive Offline Limit Exceeded. We will use a transaction Amount set to 0 and therefore we can assume the bit is set to '0' (Upper Consecutive Offline Limit not Exceeded).	
	6	Lower Cumulative Offline Limit Exceeded. We will use a Transaction Currency Code that is different from the Card's Application Currency and set the limits to 0; we therefore can assume the bit is set to '1' (Lower Cumulative Offline Limit Exceeded).	

Card Application Related Data - M/Chip 4
Generating the Authentication Token

Byte	Bit	Meaning	Carry
	5	Upper Cumulative Offline Limit Exceeded. We will use a Transaction Currency Code that is different from the Card's Application Currency and set the limits to 0; we therefore can assume the bit is set to '1' (Upper Cumulative Offline Limit Exceeded).	
	4	Go Online on Next Transaction Was Set. We can assume this bit was / is set to '1' (Go Online on Next Transaction Was Set).	
	3	Issuer Authentication Failed. We can assume this bit was / is set to '1' (Issuer Authentication Failed).	
	2	Script Received. Since we do not send Script Commands to this Card Application, this bit was / is set to '0' (No Script Received).	
	1	Script Failed. Since we do not send Script Commands to this Card Application, this bit was / is set to '0' (No Script Failed).	
6	8	RFU - Must be set to '0'	
	7	RFU - Must be set to '0'	
	6	RFU - Must be set to '0'	
	5	RFU - Must be set to '0'	
	4	RFU - Must be set to '0'	
	3	RFU - Must be set to '0'	
	2	Match Found in Additional Check Table. Since the Additional Check will not be activated, we can assume this bit being set to '0'.	
	1	No Match Found in Additional Check Table. Since the Additional Check will not be activated, we can assume this bit being set to '0'.	

Generating the Authentication Token

The Response Message returned by the M/Chip Card Application contains the following Data:

- Cryptogram Information Data.
- Application Transaction Counter
- Application Cryptogram
- Issuer Application Data / Key Derivation Index.
- Issuer Application Data / Cryptogram Version Number.
- Issuer Application Data / Card Verification Results.
- Issuer Application Data / DAC.

Card Application Related Data - M/Chip 4

Generating the Authentication Token

The Cryptogram Information Data does not need to be carried; the information is redundant with the status information in the CVR; Card Issuers can assume its value is '80' (i.e. the value indicating the Card Application returned an ARQC).

The Application Transaction Counter is needed for the Session Key Derivation; we can however carry a shorter value of the ATC and rebuild the full value at the Card Issuer side. We propose to carry 8 bits, this allows for 256 Cryptogram calculations without the Card Issuer being unable to validate the cryptogram.

The Application Cryptogram must be carried but we can shorten the information carried and have the Card Issuer to compare a portion of the calculated cryptogram with the information carried in the request. We propose to carry 16 bits; this should give sufficient confidence the Cryptogram calculated by the Card Issuer matches the Cryptogram generated by the Card Application.

The Key Derivation Index does not need to be carried - Card Issuers know what Card key derivation method is used for their cards and can find shortcuts that do not require this data element at Cryptogram Validation time.

The Cryptogram Version Number does not need to be carried - Card Issuers know what session key derivation method is used for their card and therefore do not need to carry the information.

We do not need to carry the full value of the Card Verification Results; as shown in the table we only need to carry 1 bit.

The DAC included in the response is the same value provided by the Authentication Terminal; it therefore can be set to '0' and does not need to be carried (it is not included in the Cryptogram Calculation either).

The Authentication Token is built by the terminal application; to make the application generic, MasterCard recommends the use of the Issuer Internet Proprietary Bitmap / IIPB data element to identify what bit values to select for the generation of the Authentication token.

The Response Message returned by the M/Chip Card Application contains the following Data:

- Cryptogram Information Data.
- Application Transaction Counter
- Application Cryptogram.
- Issuer Application Data / Key Derivation Index.
- Issuer Application Data / Cryptogram Version Number.
- Issuer Application Data / Card Verification Results.
- Issuer Application Data / DAC or ICC Dynamic Number.

The Cryptogram Information Data does not need to be carried; the information is redundant with the status information in the CVR; Card Issuers can assume its value is '80' (i.e. the value indicating the Card Application returned an ARQC).

60475639 . 060403

Card Application Related Data - M/Chip 4
Generating the Authentication Token

The Application Transaction Counter is needed for the Session Key Derivation; we can however carry a shorter value of the ATC and rebuild the full value at the Card Issuer side. We propose to carry 8 bits, this allows for 256 Cryptogram calculations without the Card Issuer being unable to validate the cryptogram.

The Application Cryptogram must be carried but we can shorten the information carried and have the Card Issuer to compare a portion of the calculated cryptogram with the information carried in the request. We propose to carry 16 bits; this should give sufficient confidence the Cryptogram calculated by the Card Issuer matches the Cryptogram generated by the Card Application.

The Key Derivation Index does not need to be carried - Card Issuers know what Card key derivation method is used for their cards and can find shortcuts that do not require this data element at Cryptogram Validation time.

The Cryptogram Version Number does not to be carried - Card Issuers know what session key derivation method is used for their card and therefore do not need to carry the information.

We do not need to carry the full value of the Card Verification Results; as shown in the table we only need to carry 1 bit.

The DAC included in the response is the same value provided by the Authentication Terminal; it therefore can be set to '0' and does not to be carried (it is not included in the Cryptogram Calculation either).

The Authentication Token is build by the terminal application; to make the application generic, MasterCard recommends the use of the Issuer Internet Proprietary Bitmap / IIPB data element to identify what bit values to select for the generation of the Authentication token.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

BLACK BORDERS

IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

FADED TEXT OR DRAWING

BLURRED OR ILLEGIBLE TEXT OR DRAWING

SKEWED/SLANTED IMAGES

COLOR OR BLACK AND WHITE PHOTOGRAPHS

GRAY SCALE DOCUMENTS

LINES OR MARKS ON ORIGINAL DOCUMENT

REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.